Série A, n°
N° d'ordre 803

THESES

présentées

AU CENTRE D'ORSAY

UNIVERSITE PARIS-SUD

pour obtenir

le grade de Docteur Es - Sciences

par

Denise LEGRAND

1re Thèse - FORMES QUADRATIQUES ET ALGEBRES QUADRATIQUES

2e Thèse - PROPOSITIONS DONNEES PAR LA FACULTE

Soutenue le 21 Juin 1971 devant la Commission d'Examen

Membres du Jury : MM. LESIEUR, Président
SAMUEL, Examinateur
DENY, Examinateur

Série A, n°
N° d'ordre 803

THESES

présentées

AU CENTRE D'ORSAY

UNIVERSITE PARIS-SUD

pour obtenir

le grade de Docteur Es - Sciences

par

Denise LEGRAND

1re Thèse - FORMES QUADRATIQUES ET ALGEBRES QUADRATIQUES

2e Thèse - PROPOSITIONS DONNEES PAR LA FACULTE

Soutenue le 21 Juin 1971 devant la Commission d'Examen

Membres du Jury : MM. LESIEUR, Président
SAMUEL, Examinateur
DENY, Examinateur

UNIV.
LEIDEN
BIBL.

Je tiens à exprimer ma profonde reconnaissance à Monsieur Samuel qui m'a dirigée et encouragée dans mon travail de recherche.

Je remercie Monsieur Lesieur et Monsieur Deny d'avoir accepté de faire partie du jury de cette thèse.

Je remercie Madame Bérat et Madame Lengaigne pour la rapidité et le soin apportés à la frappe du manuscrit.

INTRODUCTION

Ce travail comprend l'étude de plusieurs problèmes concernant les structures d'algèbre sur un module quadratique.

Rappel de définitions - notations.

Dans ce travail, A désigne un anneau commutatif d'unité 1. Tous les modules sont des modules unitaires. Les algèbres sont des algèbres non nécessairement associatives mais avec élément unité.

Une forme quadratique Q définie sur un A-module E est une application Q de E dans A telle que, pour tout élément X de E et tout élément a de A, $Q(aX) = a^2Q(X)$ et telle que, pour tout couple (X,X') d'éléments de E, l'application $(X,X') \mapsto Q(X+X') - Q(X) - Q(X')$ soit A-bilinéaire. Cette application est appelée la forme bilinéaire associée à Q. Sauf indication contraire, B désignera la forme bilinéaire associée à Q et B', B_0 ... etc., les formes bilinéaires associées aux formes quadratiques Q', Q_0 ... etc.

Un A-module quadratique (E,Q) est le couple formé d'un A-module E et d'une forme quadratique Q définie sur E. Tout sous-module M de E est un A-module quadratique pour la restriction de Q à M. On le note (M,Q).

Définition 0.1.1.-

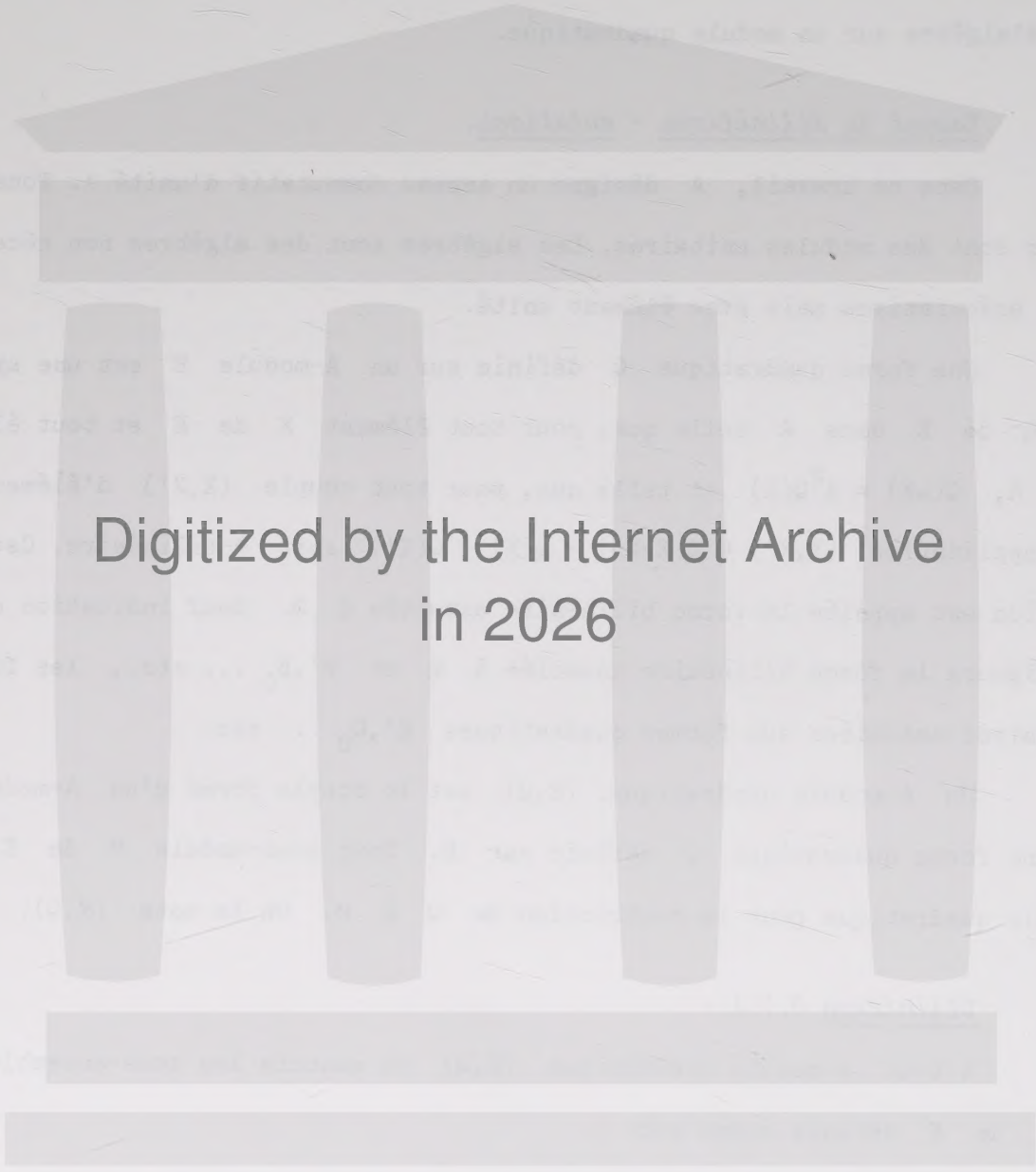
A tout A-module quadratique (E,Q) on associe les sous-ensembles H, K et K_1 de E définis comme suit :

$$H = \{X \mid X \in E \text{ et } Q(X) = 0\}$$

$$K = \{X \mid X \in E \text{ et } \forall X' \in E, B(X,X') = 0\}$$

$$K_1 = K \cap H .$$

H est l'ensemble des éléments isotropes, K_1 le noyau du module quadratique (E,Q). Lorsque 2 est régulier dans A, $K = K_1$. Par définition, Q est dégénérée si et seulement si $K \neq (0)$.



Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41550026_0050

Définition 0.1.2.-

On dit qu'une A-algèbre E d'unité e est une Q-algèbre pour une forme quadratique Q définie sur E lorsque $Q(e) = 1$ et lorsque tout élément X de E vérifie l'équation

$$X^2 + Q(X)e - B(X,e)X = 0 .$$

Ceci étant posé, on constate que toute algèbre unitaire libre ou projective, de rang 2 sur A, est une N-algèbre pour la forme norme N et que toute forme Q pour laquelle E est une Q-algèbre coïncide avec la norme.

Un premier problème se pose, le problème de la détermination des structures de Q-algèbre sur un A-module quadratique (E,Q) libre ou projectif, de rang 2 sur A. Ce problème est étudié dans les chapitres I (§1) et III (§1), (Problème 1). Un théorème d'existence et d'unicité montre en particulier que toute algèbre unitaire libre ou projective de rang 2 est déterminée à isomorphisme près par la donnée de la forme norme.

Un idéal d'une telle algèbre est un module quadratique. Un deuxième problème se pose, le problème de la détermination des structures d'idéal de Q-algèbre sur un module quadratique donné. Cette étude est faite dans le chapitre II pour les idéaux libres de rang 2 des algèbres unitaires libres de rang 2. Elle est suivie d'une application : Une correspondance entre classes d'idéaux d'une algèbre unitaire libre de rang 2 sur A et classes de formes quadratiques binaires à coefficients dans A.

Les propriétés des algèbres unitaires libres ou projectives de rang 2 et de leurs idéaux peuvent être étudiées en utilisant leur structure de module quadratique. Cette étude est faite dans les chapitres I et III (§2).

Le paragraphe § 3 du chapitre III est consacré à l'étude des algèbres unitaires sur un anneau intègre. On y voit en particulier que ces algèbres ne sont pas nécessairement des Q-algèbres et que de plus pour qu'une algèbre E d'unité e de rang 2 sur l'anneau intègre A soit une Q-algèbre pour une forme Q con-

venable, il faut et il suffit que tout élément X de E vérifie une équation de la forme $X^2 = \alpha(X)e + \beta(X)X$, $(\alpha(X) , \beta(X) \in A)$.
La forme quadratique Q est alors uniquement déterminée.

On étudie ensuite le problème 1 pour les modules quadratiques de rang 2 sur un anneau intègre.

Le chapitre IV est consacré à l'étude des Q-algèbres générales commutatives ou non. Il peut d'ailleurs arriver qu'une algèbre soit à la fois une Q-algèbre et une Q'-algèbre pour des formes Q et Q' distinctes.

Le chapitre V est consacré à l'étude des formes quadratiques multiplicatives sur les algèbres étudiées dans les chapitres précédents.

CHAPITRE I

ALGEBRES UNITAIRES LIBRES DE RANG 2 .

---

§ 1 - *Structures d'algèbre unitaire sur un A-module quadratique libre de rang 2.*

Rappels.

Soit E une A-algèbre commutative libre de rang fini.
Pour tout élément X de E, la multiplication par X est un endomorphisme du A-module E. A tout élément X de E, on associe sa norme N(X), déterminant de la multiplication par X. On définit ainsi une application N de E dans A.

Proposition 1.1.0.- (B.A. Ch. III).

Soit E une A-algèbre libre de rang 2, d'unité e.
E est associative et commutative et l'application norme N est une forme quadratique définie sur E telle que N(e) = 1. Tout élément X de E vérifie l'équation

$$X^2 = - N(X)e + B_N(X,e)X$$

où B_N est la forme bilinéaire associée à N.

Corollaire.

Toute A-algèbre unitaire E libre de rang 2 est une N-algèbre (déf. 0.1.1.) pour la norme N. Toute forme quadratique Q définie sur E pour laquelle E est une Q-algèbre coïncide avec la norme N.

En effet, d'après la définition 0.1.2., une A-algèbre d'unité e est une N-algèbre pour une forme quadratique N définie sur E lorsque N(e) = 1 et lorsque tout élément X de E vérifie l'équation $X^2 = - N(X)e + B(X,e)X$. La proposition 1.1.0. montre que E est une N-algèbre pour la norme N.

Toute A-algèbre E libre de rang 2 d'unité e possède une base contenant l'unité. Soit (e,i) une telle base et soient α et β les deux éléments

de A définis par la relation $i^2 = \alpha e + \beta i$. Alors la norme N est la forme quadratique définie par $N(e) = 1$, $N(i) = -\alpha$, $B_N(e,i) = \beta$. Il est immédiat que toute forme quadratique Q telle que E soit une Q-algèbre coïncide avec la norme N. (On a nécessairement $Q(e) = 1$, $Q(i) = -\alpha$, $B(e,i) = \beta$). On est amené à poser le problème suivant :

Problème 1.

Soit (E,Q) un A-module quadratique libre de rang 2.
Peut-on définir sur E une structure de A-algèbre unitaire telle que, N désignant la norme de l'algèbre on ait, pour tout élément X de E, $N(X) = Q(X)$?

D'après le corollaire précédent, le problème 1 peut aussi être énoncé comme suit :

Peut-on définir sur (E,Q) une structure de A-algèbre unitaire telle que E soit une Q-algèbre pour cette structure ?

1 - Théorème d'existence et d'unicité.

Théorème 1.1.1.-

Soit (E,Q) un A-module quadratique libre de rang 2.
Pour qu'il existe sur E une structure de Q-algèbre, (autrement dit pour que le problème 1 admette une solution), il faut et il suffit que la forme Q représente 1.

- Si e est l'unité d'une algèbre solution, $Q(e) = 1$.
Inversement, à tout élément e de E tel que $Q(e) = 1$, on peut faire correspondre une algèbre solution et une seule d'unité e.

- Les algèbres solutions sont isomorphes.

On utilise le lemme suivant

Lemme 1.-

Tout élément e de E tel que $Q(e) = 1$ fait partie d'une base du A-module E.

Preuve du lemme.

Soit (e_1,e_2) une base du A-module E et soit $e = m\,e_1 + n\,e_2$, $(m,n \in A)$, tel que $Q(e) = 1$. On suppose Q définie par $Q(e_1) = a$, $Q(e_2) = c$, $B(e_1,e_2) = b$. m et n vérifient la relation

$$(1) \qquad am^2 + bmn + cn^2 = 1$$

Or pour que deux éléments $m\,e_1 + n\,e_2$ et $p\,e_1 + q\,e_2$ de E, $(m,n,p,q \in A)$, forment une base de E, il suffit que $mq - pn$ soit inversible. Si on choisit par exemple $p = -cn$, $q = am + bn$, on a, compte tenu de (1), $mq - pn = 1$ et le couple $(m\,e_1 + n\,e_2 , p\,e_1 + q\,e_2)$ forme une base de E.

Preuve du théorème 1.1.1.

Pour toute solution d'unité e, $Q(e) = 1$. De plus, toute base (e,i) d'une algèbre solution d'unité e vérifie la relation $i^2 = -Q(i)e + B(e,i)i$. Il existe donc au plus une algèbre solution d'unité e.

Inversement, soit e un élément de E tel que $Q(e) = 1$. D'après le lemme, e fait partie d'une base (e,i) de E et pour la structure d'algèbre d'unité e définie par $i^2 = -Q(i)e + B(e,i)i$, la norme N coïncide avec Q, ce qui montre l'existence d'une solution associée à e.

- Donc, à tout élément e de E tel que $Q(e) = 1$ correspond une algèbre solution et on obtient ainsi toutes les solutions.

Soit E_e l'algèbre solution associée à e et soit (e,i) la base utilisée dans la preuve du lemme, $(e = m\,e_1 + n\,e_2,\ i = -cne_1 + (am + bn)e_2)$. Compte tenu de (1), $Q(i) = ac$ et $B(e,i) = b$. Comme ac et b ne dépendent pas du choix de e, les algèbres solutions associées aux différents couples (m,n) vérifiant (1) sont isomorphes.

2 - Etude des isomorphismes.

Proposition 1.1.2.-

Soit (E,Q) un A-module quadratique libre de rang 2.

On suppose qu'il existe deux éléments e et e' de E tels que $Q(e) = Q(e') = 1$ et on désigne par E_e et $E_{e'}$ les Q-algèbres solutions du problème 1 associées à e et e' respectivement. Il y a identité entre l'ensemble $\Sigma_{ee'}$ des isomorphismes d'algèbres de E_e sur $E_{e'}$ et l'ensemble des transformations orthogonales σ de (E,Q) telles que $\sigma(e) = e'$.

Preuve.

- Un isomorphisme de A-algèbres de E_e sur $E_{e'}$ conserve les normes donc est une transformation orthogonale de (E,Q).

- Inversement, soit σ une transformation orthogonale de (E,Q) telle que $\sigma(e) = e'$. Soit (e,i) une base de E. Le couple $(\sigma(e),\sigma(i))$ est une base de E et $\sigma(e)$ est l'unité de $E_{e'}$. Un calcul immédiat montre que σ est un isomorphisme de A-algèbres.

Corollaire.

Soit $O(Q)$ le groupe orthogonal de (E,Q). On suppose qu'il existe un élément e de E tel que $Q(e) = 1$. Alors les ensembles $\Sigma_{ee'}$, où e' décrit le cercle unité C de (E,Q) $(C = \{X | X \in E \text{ et } Q(X) = 1\})$ forment une partition de $O(Q)$. En particulier, $O(Q)$ opère transitivement sur le cercle unité C.

Ce corollaire est une conséquence immédiate de la proposition 1.1.2. et du fait que les ensembles $\Sigma_{ee'}$ ne sont jamais vides (Th. 1.1.1.).

Proposition 1.1.3.

Soient (E,Q) un A-module quadratique libre de rang 2, e et e' deux éléments de E tels que $Q(e) = Q(e') = 1$, E_e et $E_{e'}$ les Q-algèbres associées à e et e' respectivement, $\Sigma_{ee'}$ l'ensemble des isomorphismes d'algèbres de E_e sur $E_{e'}$ et σ_1 un élément de $\Sigma_{ee'}$. On désigne par T_e le groupe d'automorphismes de l'algèbre E_e. Alors, $\Sigma_{ee'} = \{\sigma_1 \circ \tau | \tau \in T_e\}$ et l'application $\tau \mapsto \sigma_1 \circ \tau$ est une bijection de T_e sur $\Sigma_{ee'}$.

Preuve.

Soient σ_1 et σ_2 deux éléments de $\Sigma_{ee'}$, et $\tau = \sigma_1^{-1} \circ \sigma_2$. Alors τ est l'unique élément de T_e tel que $\sigma_2 = \sigma_1 \circ \tau$.

Inversement, pour tout élément τ de T_e, $\sigma_1 \circ \tau$ est un élément de $\Sigma_{ee'}$.

Conséquence.

Un ensemble $\Sigma_{ee'}$ est parfaitement déterminé lorsqu'on connaît l'un de ses éléments et le groupe T_e.

Application.

Soit E_e une A-algèbre libre de rang 2 d'unité e, de norme N, de groupe d'automorphismes T_e. Pour tout élément e' de E_e tel que $N(e') = 1$, l'application $m_{e'} : X \to e'X$ est une transformation orthogonale de (E_e, N) telle que $m_{e'}(e) = e'$. Donc

$$O(N) = \{m_{e'} \circ \tau \mid e' \in E_e,\ N(e') = 1 \text{ et } \tau \in T_e\}$$

L'étude du groupe d'automorphismes d'une algèbre unitaire libre de rang 2 sera faite dans le paragraphe § 2.

§ 2 - *Etude d'une algèbre unitaire libre de rang 2.*

Selon la terminologie de B.A. Ch. III une algèbre quadratique est par définition une algèbre unitaire libre de rang 2. On utilisera ici cette terminologie.

Dans tout ce paragraphe, E désigne une algèbre quadratique sur A d'unité e, de norme N. On désigne par B la forme bilinéaire associée à N.

Pour tout élément X de E, N(X), (resp. B(X,e)), est le déterminant, (resp. la trace), de l'endomorphisme $m_X : Y \to XY$ du A-module E.

1 - Propriétés préliminaires.

Proposition 1.2.1.

La norme N de l'algèbre quadratique E est multiplicative sur E et

l'application σ définie sur E par $\sigma(X) = B(X,e)e - X$ est un automorphisme de l'algèbre E tel que, pour tout élément X de E, $X\,\sigma(X) = N(X)e$.

Preuve (voir aussi B.A. Ch. III)

- Pour tout couple (X,X') d'éléments de E, $m_X \circ m_{X'} = m_{XX'}$ donc $N(X)N(X') = \det(m_X)\det(m_{X'}) = \det(m_{XX'}) = N(XX')$.

- Il est immédiat que σ est une transformation orthogonale de (E,N) telle que $\sigma(e) = e$. C'est donc un automorphisme de l'algèbre E (prop. 1.1.2.). La dernière égalité est une conséquence de l'équation $X^2 = - N(X)e + B(X,e)X$.

Corollaire 1.

Pour qu'un élément X de l'algèbre quadratique E soit inversible il faut et il suffit que N(X) soit un élément inversible de A.

En effet, si X est inversible, il existe un élément X' de E tel que $XX' = e$, $N(X)N(X') = N(XX') = 1$. Donc N(X) est inversible dans A.

Inversement, lorsque N(X) est inversible, l'élément $\frac{\sigma(X)}{N(X)}$ est l'inverse de X dans E.

Corollaire 2.

Pour qu'un élément X de E soit régulier, il faut et il suffit que N(X) soit un élément régulier de A.

En effet : soit X un élément de E.

- Lorsque N(X) n'est pas régulier, il existe $a \in A - \{0\}$ tel que $a(X\,\sigma(X)) = a\,N(X)e = 0$. On a donc $X\,\sigma(aX) = 0$ et ou bien $\sigma(aX) \neq 0$ ou bien $(ae)X = aX = 0$ puisque σ est injectif. Donc X n'est pas régulier.

- Pour tout élément X' de E tel que $XX' = 0$, $N(X)X' = (X\,\sigma(X))X' = 0$. Lorsque N(X) est régulier, $N(X)X' = 0$ implique $X' = 0$ puisque E est libre. Donc X est régulier.

Corollaire 3.

Pour que E soit égal à son anneau total de fractions, il faut et il

suffit que A soit égal à son anneau total de fractions.

Preuve.

Lorsque A est égal à son anneau total de fractions, il en est de même pour E. C'est une conséquence directe des deux corollaires précédents.

Inversement, on suppose que E est égal à son anneau total de fractions. Soit a un élément de A, alors $N(ae) = a^2$ et on a la chaîne d'implications suivante :

a régulier dans A $\Longrightarrow$ N(ae) régulier

N(ae) régulier $\Longrightarrow$ ae régulier dans E (cor. 2)

ae régulier dans E $\Longrightarrow$ ae inversible dans E

ae inversible dans E $\Longrightarrow$ a^2 inversible dans A (cor. 1)

Donc tout élément régulier de A est inversible.

2 - Propriétés relatives à l'ensemble des éléments isotropes et au noyau du module quadratique (E,N).

On associe à (E,N) les ensembles suivants (Introduction déf. 0.1.1.)

$$H = \{X | X \in E \text{ et } N(X) = 0\}$$

$$K = \{X | X \in E \text{ et } \forall X' \in E, B(X,X') = 0\}$$

$$K_1 = K \cap H$$

H est l'ensemble des éléments isotropes et K_1 le noyau du module quadratique (E,N). Lorsque 2 est régulier, $K = K_1$. Par définition N est dégénérée si et seulement si $K \neq \{0\}$.

a) Détermination et étude des ensembles H, K, K_1 .

Soit (e,i) une base de E telle que $i^2 = \alpha e + \beta i$, ($N(i) = -\alpha$, $B(e,i) = \beta$

K est l'ensemble des éléments xe + yi de E tels que :

(1) $2x + \beta y = 0$ $\qquad$ $(B(xe + yi,e) = 0)$

$\beta x - 2\alpha y = 0$ $\qquad$ $(B(xe + yi,i) = 0)$

Donc N est dégénérée si et seulement si $4\alpha + \beta^2$ est un élément non régulier de A.

K_1 est l'ensemble des éléments $xe + yi$ de K vérifiant

(3) $\quad x^2 + \beta xy - \alpha y^2 = 0 \qquad (N(xe + yi) = 0)$

Proposition 1.2.2.-

K et K_1 sont des idéaux de E.

Preuve.

Il est immédiat que K et K_1 sont des sous A-modules de E. D'autre part, $\forall\, X \in K$, $\forall\, X' \in E$, $XX' \in K$.

En effet, soit (e,i) une base de E telle que $i^2 = \alpha e + \beta i$.
Si $X = xe + yi$ et $X' = x'e + y'i$, $XX' = (xx' + \alpha yy')e + (xy' + x'y + \beta yy')i$
$B(XX',e) = 2(xx' + \alpha yy') + \beta(xy' + x'y + \beta yy') = B(X,e)x' + B(X,i)y' + (4\alpha + \beta^2)yy'$
$B(XX',i) = \beta(xx' + \alpha yy') - 2\alpha(xy' + x'y + \beta yy') = B(X,i)x' - B(X,e)\alpha y'$. Lorsque X appartient à K, $B(X,e) = B(X,i) = 0$ et puisque x et y vérifient les équations (1) et (2) , $(4\alpha + y^2)y = 0$. Donc $B(XX',e) = 0$, $B(XX',i) = 0$ et XX' appartient à K.

Lorsque de plus X appartient à K_1 , $N(XX') = N(X)N(X') = 0$ donc XX' appartient à K_1.

Proposition 1.2.3.-

Tout élément du noyau K_1 est de carré nul.

Lorsque 2 est régulier dans A, $K_1^2 = K^2 = (0)$.

Preuve.

Pour tout élément X de E, $X^2 = -N(X)e + B(X,e)X$ et pour tout couple (X,X') d'éléments de E

$2XX' = (X + X')^2 - X^2 - X'^2 = -B(X,X')e + B(X,e)X' + B(X',e)X$.

Donc, lorsque X appartient à K_1 , $X^2 = 0$ et lorsque X et X' appartiennent à K_1 , $2XX' = 0$. Lorsque 2 est régulier dans A, $K = K_1$ et pour tout couple (X,X') d'éléments de K, $XX' = 0$.

b) Propriétés liées aux ensembles H, K et K_1.

Il résulte de a) que K_1 est un idéal de E contenu dans le nilradical de E. Lorsque K_1 n'est pas nul, E n'est pas réduit. On va étudier quelques cas particuliers.

1°) On suppose A réduit

Proposition 1.2.4.-

Lorsque A est réduit le nilradical de E est l'ensemble des éléments X de E tels que $N(X) = B(X,e) = 0$. C'est donc l'ensemble des éléments de carré nul. Cet ensemble est égal au noyau K_1 de (E,N).

Preuve.

- Pour qu'un élément X de E soit nilpotent, il faut et il suffit que $N(X) = B(X,e) = 0$. En effet, pour tout élément X de E

$$X^2 = - N(X)e + B(X,e)X$$

donc

$$(B(X,e) = 0 \text{ et } N(X) = 0) \implies X^2 = 0 .$$

Inversement, on suppose qu'il existe $n \in N - \{0\}$ tel que $X^n = 0$. Puisque N est multiplicative et A réduit, $N(X^n) = 0$ implique $N(X) = 0$. On en déduit successivement :

$X^2 = B(X,e)X$, $X^n = (B(X,e))^{n-1}X$, $0 = B(X^n,e) = B((B(X,e)^{n-1}X,e) = (B(X,e))^n$, $B(X,e) = 0$.

Il en résulte que tout élément nilpotent est de carré nul.

Pour montrer que tout élément de carré nul appartient à K_1 il suffit de

montrer que tout élément X de E qui vérifie les conditions $N(X) = 0$ et $B(X,e) = 0$ vérifie aussi la condition $B(X,i) = 0$.

Soit $X = xe + yi$, $(x,y \in A$; (e,i), base de E telle que $i^2 = \alpha e + \beta i)$

$N(X) = x^2 + \beta xy - \alpha y^2$, $B(X,e) = 2x + \beta y$, $B(X,i) = \beta x - 2\alpha y$.

On en déduit

(4) $\quad 4\alpha N(X) = (2\alpha y - \beta x)^2 - (4\alpha + \beta^2)x^2$

(5) $\quad 4N(X) = (2x + \beta y)^2 - (4\alpha + \beta^2)y^2$

On suppose que $B(X,e) = 0$ et $N(X) = 0$.

Puisque $B(X,e) = 2x + \beta y = 0$, $N(X) = -(x^2 + \alpha y^2)$.

Puisque $N(X) = 0$ et $B(X,e) = 0$, $x^2 = -\alpha y^2$ et $(4\alpha + \beta^2)y^2 = 0$.

On en déduit $(4\alpha + \beta^2)x^2 = 0$, $(2\alpha y - \beta x)^2 = 0$ et puisque A est réduit, $-2\alpha y + \beta x = 0$ c'est-à-dire $B(X,i) = 0$.

Corollaire.

On suppose A réduit, alors :

- E est réduit si et seulement si $K_1 = (0)$.
- Lorsque 2 est régulier, E est réduit si et seulement si N n'est pas dégénérée.

2°) On suppose A intègre

Proposition 1.2.5.-

On suppose A intègre, alors :

- H est l'ensemble des éléments non réguliers de E.
- Lorsque N est dégénérée, $H = K_1$ et H est un idéal premier qui est le nilradical de E.

Preuve.

- H est l'ensemble des éléments non réguliers de E. C'est une consé-

quence du corollaire 2 de la proposition 1.2.1.

On reprend la base (e,i) de la preuve précédente, $(i^2 = \alpha e + \beta i)$.

- Lorsque N est dégénérée, $4\alpha + \beta^2 = 0$.

Soit X un élément de H, $X = xe + yi$. Selon (4) et (5)

$$4\alpha N(X) = (\beta x - 2\alpha y)^2 - (4\alpha + \beta^2)x^2$$

$$4N(X) = (2x + \beta y)^2 - (4\alpha + \beta^2)y^2$$

Donc,

$$(N(X) = 0 \text{ et } 4\alpha + \beta^2 = 0) \Longrightarrow (2x + \beta y = \beta x - 2\alpha y = 0) .$$

Ce qui montre que H est inclus dans K. Donc $H = K_1$ et d'après la proposition 1.2.4., H est égal au nilradical de E. H est un idéal premier car $N(XX') = 0$ implique $N(X) = 0$ ou $N(X') = 0$.

Remarques (On suppose toujours A intègre).

1) Lorsque K_1 n'est pas nul, pour tout idéal non nul I de E, $I \cap K_1 \neq (0)$. En effet, si I est contenu dans K_1, $I \cap K_1 \neq (0)$. Sinon, il existe $X \in I - K_1$. X est régulier car $H = K_1$ donc si X_1 est un élément non nul de K_1, $XX_1 \in I \cap K_1$ et $XX_1 \neq 0$.

2) Lorsque N est dégénérée, tout élément non régulier de E est de carré nul (car $H = K_1$).

3) On suppose A principal.

Les idéaux de E sont libres de rang 2 au plus.

Proposition 1.2.6.-

On suppose A principal. Alors les idéaux de rang 1 de l'algèbre E sont les idéaux non nuls contenus dans H. Ce sont les sous-modules monogènes de E engendrés par les éléments de $H - \{0\}$.

Preuve.

On reprend la base (e,i) de E. $(i^2 = \alpha e + \beta i, \alpha, \beta \in A)$

- De façon générale, même lorsque A n'est pas intègre, tout idéal libre de rang 2 contient un élément de E-H. En effet, si (e_1,e_2) est une base d'un tel idéal I, le déterminant δ de (e_1,e_2) relatif à (e,i) est un élément régulier de A et δe est un élément de I de norme δ^2 non nulle.

On suppose maintenant A principal. Soit $A\,e_1$ le sous A-module de E de base e_1. Pour que $A\,e_1$ soit un idéal de E, il faut et il suffit que $i\,e_1$ appartienne à $A\,e_1$.

Si $e_1 = me + ni$, $ie_1 = n\alpha e + (m + n\beta)i$. Alors,

$$(i\,e_1 \in A\,e_1) \iff (\exists\, k \in A \mid n\alpha = km \text{ et } m + n\beta = kn) .$$

Pour que le système $(n\alpha = km,\ m + n\beta = kn)$ admette une solution k dans A, il faut et il suffit que $m^2 + mn\beta - \alpha n^2 = 0$ et que n divise m. Mais puisque A est principal, pour tout couple (m,n) tel que n soit $\neq 0$ et $m^2 + mn\beta - \alpha n^2 = 0$, n divise m. En effet, A est intégralement clos et $\frac{m}{n}$ est solution dans le corps des fractions de A d'une équation entière à coefficients dans A.

En définitive, pour que le A-module $A\,e_1$ soit un idéal de E, il faut et il suffit que $m^2 + mn\beta - \alpha n^2 = 0$ c'est-à-dire que $N(e_1) = 0$.

Corollaire.

Lorsque A est principal, le produit de deux idéaux de E libres de rang 2 est un idéal libre de rang 2.

En effet, ce produit contient un élément $\delta\delta' e$ où δ et δ' sont réguliers.

On peut distinguer trois cas auxquels correspondent trois types d'anneaux E.

Cas 1. $H = \{0\}$.

E est intègre. Les idéaux non nuls de E sont des A-modules libres de rang 2.

Cas 2. $H \neq \{0\}$, $K = K_1 = (0)$.

E n'est pas intègre, il est réduit. Les idéaux de rang 1 se répartissent en deux familles. Ce sont les idéaux de la forme λI_1 ou λI_2 , $(\lambda \in A - \{0\})$, où I_1 et I_2 sont tels que $I_1 \cap I_2 = (0)$ $I_1 \cup I_2 = H$. H n'est pas un idéal.

En effet, puisque H n'est pas nul, l'équation $x^2 + \beta xy - \alpha y^2 = 0$ admet au moins une solution (x,y) avec $y \neq 0$. Par un raisonnement analogue au précédent, on voit que pour une telle solution, $\frac{x}{y}$ appartient à A. Compte tenu du fait que $K = (0)$, $(4\alpha + \beta^2 \neq 0)$, il existe exactement deux valeurs pour $\frac{x}{y}$. Si on les désigne par a_1 et a_2, les idéaux I_1 et I_2 de bases respectives $a_1 e + i$, $a_2 e + i$, vérifient les propriétés indiquées. Cela résulte de la proposition 1.2.6. puisque les éléments de norme nulle sont de la forme $\lambda(a_1 e + i)$ ou $\lambda(a_2 e + i)$, $(\lambda \in A)$.

Cas 3. $K_1 \neq (0)$.

$H = K_1$, (prop. 1.2.5.)

E n'est pas réduit. Les idéaux de rang 1 sont les idéaux λK_1 , $(\lambda \in A - \{0\})$.

Le raisonnement est analogue au précédent.

Plus particulièrement, lorsque A est un corps.

Cas 1. E est un corps.

Cas 2. E possède exactement deux idéaux stricts non nuls I_1 et I_2. Ces idéaux sont maximaux et possèdent les propriétés indiquées plus haut.

Cas 3. E possède un seul idéal, le noyau K_1.

On déduit de cette étude quelques propriétés des idéaux de E lorsque A est seulement supposé intègre.

On suppose donc simplement A intègre.

Soient A_0 le corps des fractions de A et $E_0 = E \otimes_A A_0$. E_0 est muni de la structure d'algèbre quadratique sur A_0 obtenue par extension des scalaires à A_0. On identifie A et E à leurs images respectives dans A_0 et E_0 par les

injections canoniques. La norme N sur E est la restriction à E de la norme N_0 sur E_0.

On affecte de l'indice 0 les parties de E_0 définies de façon analogue aux parties correspondantes de E. Par exemple, H_0 désigne l'ensemble des éléments isotropes de E_0. Il est immédiat que H_0 (resp. K_0, resp. $K_{1,0}$), est l'extension de H, (resp. K, resp. K_1), que $H = H_0 \cap E$, $K = K_0 \cap E$, $K_1 = K_{1,0} \cap E$.

Soit I un idéal de E, son extension I_0 est un idéal de E_0. On obtient les résultats suivants :

Cas 1. $H = \{0\}$

E est intègre; les idéaux non nuls sont de rang 2.

Cas 2. $H \neq \{0\}$, $K = K_1 = (0)$.

E n'est pas intègre, il est réduit. Les idéaux de rang 1 sont les idéaux $\neq (0)$ contenus dans H et se répartissent en deux familles comme suit. Il existe deux idéaux de rang 1 I_1 et I_2 tels que $I_1 \cap I_2 = (0)$, $I_1 \cup I_2 = H$, les idéaux de rang 1 sont les idéaux contenus soit dans I_1, soit dans I_2.

I_1 et I_2 sont les idéaux premiers ($I_1 = I_{1,0} \cap E$, $I_2 = I_{2,0} \cap E$, où $I_{1,0}$ et $I_{2,0}$ sont les deux idéaux stricts $\neq (0)$ de E_0).

H n'est pas un idéal.

Cas 3. $K_1 \neq (0)$

E n'est pas réduit. Les idéaux de rang 1 sont les idéaux $\neq (0)$ contenus dans le nilradical K_1.

Remarque. On a déjà vu que dans le cas 3, chaque idéal $\neq (0)$ a une intersection non nulle avec K_1 (preuve de la proposition 1.2.5. remarque 1). Un raisonnement analogue montre que dans le cas 2 chaque idéal $\neq (0)$ a une intersection non nulle avec I_1 ou avec I_2.

3 - Etude du groupe d'automorphismes de l'algèbre quadratique E.

Soit (e,i) une base de E telle que $i^2 = \alpha e + \beta i$, ($N(i) = -\alpha$, $B(e,i) = \beta$). D'après la proposition 1.1.2., les automorphismes de l'algèbre E

sont les transformations orthogonales de (E,N) qui laissent e invariant.

Un automorphisme σ de E est défini par la donnée d'un élément j de E, $(j = \sigma(i))$, tel que (e,j) soit une base de E et que $N(j) = N(i)$, $B(e,j) = B(e,i)$.

Soit $j = xe + yi$, $(x,y \in A)$, les conditions précédentes s'écrivent

$$\left.\begin{array}{ll} (6) & y \text{ est inversible} \\ (7) & x^2 + \beta xy - \alpha y^2 = -\alpha \\ (8) & 2x + \beta y = \beta \end{array}\right\} \qquad (1.2.7)$$

La matrice de l'automorphisme associé à une solution (x,y) est, relativement à la base (e,i),

$$\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix}$$

Le système (1.2.7) admet toujours en particulier les solutions $(x,y) = (0,1)$ et $(x,y) = (\beta,-1)$. Ces solutions sont confondues lorsque $2 = \beta = 0$. A la première correspond l'automorphisme identique, à la seconde l'automorphisme $X \to B(X,e)e - X$ déjà signalé.

a) Etude générale.

Proposition 1.2.8.-

Le groupe d'automorphismes T de E n'est pas nécessairement commutatif. L'anneau d'invariants contient Ae mais l'inclusion peut être stricte.

Lorsque 2 est régulier dans A, T est commutatif et l'anneau d'invariants est Ae. Il en est de même lorsque E possède une base (e,i) telle que $B(e,i)$ soit régulier.

Preuve.

Soient σ et σ' les automorphismes associés à deux solutions (x,y)

et (x',y') du système (1.2.7.). Pour que $\sigma \circ \sigma' = \sigma' \circ \sigma$, il faut et il suffit que

$$\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \begin{pmatrix} 1 & x' \\ 0 & y' \end{pmatrix} = \begin{pmatrix} 1 & x' \\ 0 & y' \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix}$$

c'est-à-dire que $x'(y-1) = x(y'-1)$.

- Exemple de groupe T non commutatif.

On prend pour A l'extension quadratique de l'anneau de séries formelles $k[[t]]$ sur le corps k à deux éléments définie par $A = k[[t]] \oplus k[[t]]u$ avec $u^2 = 0$, et pour algèbre E, une A-algèbre de base (e,i) telle que $i^2 = 0$ $(\alpha = \beta = 0)$.

Les couples $(x,y) = (u,y)$ avec y inversible et $(x',y') = (0,1+t)$ sont des solutions de (1.2.7.) mais $x'(y-1) = 0$ et $x(y'-1) = ut$ avec $ut \neq 0$.

- Il est évident que l'anneau d'invariants contient Ae.

Exemple d'inclusion stricte.

On prend $A = \mathbb{Z}/6\mathbb{Z}$, $\alpha = \beta = 0$. Les automorphismes de E sont associés aux couples $(0,b)$ où $b = \bar{1}$, $\bar{3}$ ou $\bar{5}$. L'élément $\bar{3}i$ est invariant par T et n'appartient pas à Ae.

- On suppose maintenant que l'un des éléments 2 ou β est régulier.

Pour tout couple de solutions $((x,y),(x',y'))$ du système (1.2.7.) $2x + \beta y = \beta$, $2x' + \beta y' = \beta$ ce qui implique

$$2\left[x'(y-1) - x(y'-1)\right] = 0 \quad \text{et} \quad \beta\left[x'(y-1) - x(y'-1)\right] = 0$$

et par suite $x'(y-1) = x(y'-1)$. Donc T est commutatif.

L'automorphisme $\sigma : X \to B(X,e)e - X$ ne laisse invariants que les éléments de Ae. En effet :

Soit $X = xe + yi$, $\sigma(X) = (x + \beta y)e - yi$ donc $\sigma(X) = X$ si et seulement si $\beta y = 2y = 0$, c'est-à-dire si et seulement si X appartient à Ae.

Remarques.

1. La condition "2 ou β régulier" n'est pas nécessaire. On verra des exemples dans la suite.

2. Lorsque 2 est régulier, il y a au plus un automorphisme de déterminant y fixé.

Etude de sous-groupes de T.

Les éléments de T de déterminant +1, (resp. -1), sont associés aux solutions du système $(x^2 + \beta x = 0,\ 2x = 0,\ y = 1)$, (resp. $(x^2 - \beta x = 0,\ 2(x-\beta) = 0,\ y = -1)$.

On voit facilement que ces éléments sont d'ordre 2 au plus et forment un sous-groupe commutatif de T. Lorsque 2 est régulier, ce sous-groupe a exactement deux éléments.

Ce sous groupe contient le groupe G des éléments de déterminant 1.

Application. Etude du groupe SO(N) du module quadratique (E,N) défini par l'algèbre E.

SO(N) est le sous-groupe de O(N) formé des éléments de déterminant 1. Puisque $O(N) = \{m_{e'} \circ \tau \mid e' \in E,\ N(e') = 1 \text{ et } \tau \in T\}$, (application de la proposition 1.1.3.),

$$SO(N) = \{m_{e'} \circ \tau \mid e' \in E,\ N(e') = 1 \text{ et } \tau \in G\}$$

SO(N) est engendré par les sous-groupes commutatifs G et M où $M = \{m_{e'} \mid e' \in E \text{ et } N(e') = 1\}$, il est réduit à M lorsque 2 est régulier, (dans ce cas G ne contient que l'identité).

Le centre de SO(N) contient le sous groupe M_1 des éléments $m_{e'}$ de M tels que e' soit invariant par G et le sous-groupe G_1 formé des éléments τ de G qui laissent fixes les éléments de norme 1. C'est le produit direct de ces deux sous-groupes. En effet :

$$\forall\, m_{e'_1} \in M_1\ ,\ \forall\, m_{e'} \circ \tau \in SO(N)\ ,\ \forall\, x \in E\ ,$$

$(m_{e'_1} \circ (m_{e'} \circ \tau))(X) = e'_1 e'\tau(X) = e'\tau(e'_1)\tau(X) = e'\tau(e'_1 X) = ((m_{e'} \circ \tau) \circ m_{e'_1})(X)$

de même, $\forall\, \tau_1 \in G_1$, $\forall\, m_{e'} \circ \tau \in SO(N)$, $\forall\, X \in E$,

$(\tau_1 \circ (m_{e'} \circ \tau))(X) = \tau_1(e'\tau(X)) = e'(\tau_1 \circ \tau)(X)) = e'(\tau \circ \tau_1)(X) = ((m_{e'} \circ \tau) \circ \tau_1(X$

Donc M_1 et G_1 sont contenus dans le centre de $SO(N)$. Il est immédiat que l'ensemble $\{m_{e'_1} \circ \tau_1 ; m_{e'_1} \in M_1 , \tau_1 \in G_1\}$ est un groupe commutatif produit direct des sous-groupes M_1 et G_1 et contenu dans le centre de $SO(N)$.

Inversement, soit $m_{e'} \circ \tau$ un élément du centre de $SO(N)$.

Pour tout élément e'' de E, de norme 1,

$((m_{e'} \circ \tau) \circ m_{e''})(e) = (m_{e''} \circ (m_{e'} \circ \tau))(e)$ c'est-à-dire $e'\tau(e'') = e''e'$.

Puisque e' est inversible (prop. 1.2.1., cor. 1), $\tau(e'') = e''$. Donc τ appartient à G_1.

Pour tout élément τ'' de G,

$((m_{e'} \circ \tau) \circ \tau'')(e) = (\tau'' \circ (m_{e'} \circ \tau))(e)$ c'est-à-dire $e' = \tau''(e')$ donc e' appartient à M_1.

b) Etude du groupe T dans des cas particuliers.

1°) On suppose A intègre.

H, K, K_1 sont définis comme dans le début de § 2 (déf. 2.1.1.).

Proposition 1.2.9.-

On suppose A intègre.

- Lorsque $K = (0)$, (N non dégénérée), le groupe d'automorphismes T de E a exactement deux éléments, l'identité et l'automorphisme $X \mapsto B(X,e)e - X$.

- Lorsque $K \neq (0)$, (N dégénérée), pour tout élément i de E tel que (e,i) soit une base de E, l'orbite O_i est l'ensemble

$O_i = \{j \mid j \in E , j = i + x_1 e + y_1 i , x_1 e + y_1 i \in K_1$ avec $1 + y_1$ inversible$\}$

Dans les deux cas le groupe T est commutatif.

Preuve.

Soit $i \in E$ tel que (e,i) soit une base de E et $i^2 = \alpha e + \beta i$, $(\alpha,\beta \in A)$.

Lorsque $K = (0)$, $(4\alpha + \beta^2 \neq 0)$, le système (1.2.7.), p. 18, a exactement deux solutions $(0,1)$ et $(\beta,-1)$. Il leur correspond l'identité et l'automorphisme $X \to B(X,e)e - X$.

On suppose maintenant que $K \neq (0)$, $(4\alpha + \beta^2 = 0)$.

Soient $X_1 = x_1 e + y_1 i$ et $j = i + X_1$

$$X_1 \in K_1 \implies (N(i + X_1) = N(i) \text{ et } B(e,i + X_1) = B(e,i)).$$

Donc ($X_1 \in K_1$ et $1 + y_1$ inversible) $\implies i + X_1 \in O_i$. Il reste à établir l'implication opposée. Lorsque $i + X_1$ appartient à O_i, $(e,i + X_1)$ est une base de E donc $1 + y_1$ est inversible. Puisque A est intègre et N dégénérée, $K_1 = H$ (prop. 1.2.5.), il suffit de montrer que $N(j-i) = 0$.

$$B(e,j) = B(e,i) \implies B(e,j-i) = 0$$

$$B(e,j-i) = 0 \implies 4\,N(j-i) = 0$$

En effet, $4N(j-i) = (B(e,j-i))^2 - (4\alpha + \beta^2)y_1^2$ et $4\alpha + \beta^2 = 0$.

Donc, lorsque $2 \neq 0$, $N(j-i) = 0$.

Lorsque $2 = 0$, $\beta = 0$ et l'équation $N(j) = N(i)$ s'écrit

$$x_1^2 - \alpha((y_1 + 1)^2 - 1) = 0$$

ou encore, puisque $2 = 0$

$$x_1^2 - \alpha\, y_1^2 = 0$$

c'est-à-dire $N(j-i) = 0$.

Conséquence.

Lorsque N est dégénérée, on a pour tout élément X de E, $(X = xe + yi)$

$O_X = \{X' \mid X' \in E,\ X' = X + y(x_1 e + y_1 i),\ x_1 e + y_1 i \in K_1 \text{ avec } 1 + y_1 \text{ inversible}\}$

- Pour montrer que T est commutatif, il suffit de montrer que cette propriété est vraie lorsque A est un corps.

En effet, on a déjà vu que E se plonge dans l'algèbre E_0 obtenue par extension des scalaires au corps des fractions A_0 de A. Tout automorphisme de l'algèbre E se prolonge en un automorphisme de E_0. Donc lorsque le groupe d'automorphismes T_0 de E_0 est commutatif, T est commutatif.

On suppose maintenant que A est un corps et on reprend l'étude des trois cas envisagés précédemment.

Cas 1. $H = \{0\}$

Lorsque $K = (0)$, T a deux éléments.

Lorsque $K \neq (0)$, T a un seul élément car N est dégénérée et $K_1 = (0)$.

Cas 2. $H = \{0\}$, $K = (0)$.

T a deux éléments, il est facile de voir que l'automorphisme $X \mapsto B(X,e)e - X$ échange les deux idéaux de E.

Cas 3. $K_1 \neq (0)$.

Soit X_0 un générateur de K_1 , $X_0 = x_0 e + y_0 i$.

$O_i = \{X' | X' \in E \ , \ X' = i + \mu X_0 \ , \ \mu \in A \ , \ 1 + \mu y_0 \neq 0\}$.

Soient σ_1 et σ_2 les automorphismes associés à μ_1 et μ_2 et $X = xe + yi$ un élément de E.

$$\sigma_1(X) = X + y\mu_1(x_0 e + y_0 i)$$

$$(\sigma_2 \circ \sigma_1)(X) = X + y[\mu_1 x_0 + \mu_2 x_0 + \mu_1\mu_2 x_0 y_0]e + yy_0[\mu_1 + \mu_2 + \mu_1\mu_2]i$$

donc $(\sigma_2 \circ \sigma_1)(X) = (\sigma_1 \circ \sigma_2)(X)$.

Le groupe T est donc commutatif.

D'autre part, K_1 est globalement invariant par T mais aucun élément de $K_1 - \{0\}$ n'est invariant par T. En effet, l'anneau d'invariants est égal à Ae car lorsque $y \neq 0$ et $\mu \neq 0$ $X + y\mu X_0 \neq X$.

On en déduit les résultats suivants lorsque A est seulement supposé intègre.

Le groupe T est commutatif.

Dans le cas 2, l'automorphisme $X \mapsto B(X,e)e - X$ transforme tout idéal de rang 1 de l'une des deux familles en un idéal de l'autre famille.

Dans le cas 3, les propriétés relatives à K_1 sont les mêmes que lorsque A est un corps.

2°) On suppose que 2 est un élément inversible de A.

Par un changement de base, on peut se ramener au cas où $\beta = 0$. On va donc supposer que $\beta = 0$.

Les solutions du système (1.2.7.) (p. 18), sont les couples $(0,y)$ tels que y soit inversible et $\alpha(y^2-1) = 0$. En particulier, lorsque N n'est pas dégénérée, (α régulier), le groupe T est isomorphe au groupe des éléments y de A tels que $y^2 = 1$. Lorsque $\alpha = 0$, T est isomorphe au groupe des éléments inversibles de A.

4 - Problèmes d'orthogonalité.

On considère le module quadratique libre de rang 2 (E,N) sous-jacent à l'algèbre E. Le sous-module Ae de E est isomorphe à A. En effet, e fait partie d'une base. De plus,

Proposition 1.2.10.-

Pour que (E,N) soit la somme directe de Ae et de l'orthogonal $(Ae)^{\perp}$ de Ae, il faut et il suffit que la propriété

(1.2.10) : (2 est régulier dans A et, $\forall$ X et X' $\in$ E , $B(X,X') \in 2A$) soit vérifiée.

(La propriété (1.2.10) est vérifiée en particulier lorsque 2 est un élément inversible de A).

Preuve.

Soit (e,i) une base de E, la propriété (1.2.10) est vérifiée si et

seulement si 2 est régulier et $B(e,i)$ multiple de 2.

On pose $B(e,i) = \beta$ comme plus haut.

- Lorsque 2 n'est pas régulier, $Ae \cap (Ae)^{\perp} \neq \{0\}$. En effet, il existe un élément x de $A - \{0\}$ tel que $2x = 0$, xe est alors un élément non nul de $Ae \cap (Ae)^{\perp}$.

Lorsque β n'est pas multiple de 2, $Ae + (Ae)^{\perp} \neq E$.
En effet, soit $X = xe + i$. Il n'existe pas d'élément a de A tel que $X - ae$ soit orthogonal à Ae, il faudrait pour cela que $2(x-a) + \beta = 0$.

- Inversement, lorsque β est un multiple de 2, $(\beta = 2\beta')$, le couple $(e, i-\beta'e)$ est une base de E telle que $B(e,i-\beta'e) = 0$. $E = Ae \oplus A(i-\beta'e)$. Lorsque de plus 2 est régulier, $A(i-\beta'e) = (Ae)^{\perp}$.

Proposition 1.2.11.-

On suppose que l'anneau A et le module (E,N) sous-jacent à l'algèbre E vérifient la propriété (1.2.10). Alors,

- Les idéaux de E contenus dans $(Ae)^{\perp}$ sont les sous-modules de E contenus dans le noyau K_1 de (E,N).

- Les idéaux de E contenus dans Ae sont les sous A-modules de $\mathfrak{a}e$ où $\mathfrak{a}$ désigne l'annulateur de $(Ae)^{\perp}$.

Preuve.

On pose $(Ae)^{\perp} = M$. Le noyau K_1 de (E,N) est un idéal de E (prop. 1.2.2) il est immédiat qu'il est contenu dans M.

- Soit I un sous A-module de M contenu dans K_1 et soit X un élément de I. Pour tout élément $ae + Y$ de E, $(a \in A, Y \in M)$,

$$2X(ae + Y) = - B(X,ae + Y)e + B(X,e)(ae + Y) + B(ae + Y,e)X = 2aX .$$

Puisque 2 est régulier et E libre, $X(ae + Y) = aX$. Donc I est un idéal de E. Inversement, soit I un idéal de E contenu dans M et soit X un élément de I. Pour tout élément $ae + Y$ de E $(a \in A , Y \in M)$,

$2X(ae + Y) = 2aX - B(X,Y)e + B(X,e)Y + B(y,e)X = 2aX - B(X,Y)e.$

Puisque $2aX - B(X,Y)e$ est un élément de M, $B(X,Y) = 0$. Donc X appartient à M.

- Soient I un sous A-module de α et X un élément de I. Pour tout élément $ae + Y$ de E, $(a \in A , Y \in M)$, $X(ae + Y) = aX$. Donc I est un idéal.

Inversement, soient I un idéal contenu dans Ae et $a'e$ un élément de I. Pour tout élément Y de M, $XY = a'Y$ et $XY \in Ae$. Donc $a'Y = 0$ et $a' \in \alpha$.

On peut remplacer la propriété (1.2.10) par une propriété moins restrictive et obtenir une décomposition du même type.

Proposition 1.2.10'.-

(E,N) désignant le module sous-jacent à l'algèbre quadratique E d'unité e, de norme N, on suppose que la propriété suivante est vérifiée.

(1.2.10)' Il existe une forme bilinéaire B_1 définie sur E^2 telle que, pour tout élément X de E, $N(X) = B_1(X,X)$.

Alors E admet la décomposition $E = Ae \oplus (Ae)^{\perp_1}$ où $(Ae)^{\perp_1}$ est l'orthogonal de Ae pour la forme bilinéaire B_1.

- Pour tout couple (X,X') d'éléments de E,

$$XX' = - B_1(X,X')e + B_1(X,e)X' + B_1(X',e)X$$

En effet, il est immédiat que Ae et $(Ae)^{\perp_1}$ sont des sous-modules de E d'intersection nulle et que tout élément X de E se met sous la forme $X = B_1(X,e)e + Y$ où Y appartient à $(Ae)^{\perp_1}$; (e,i) désignant une base de E, $(Ae)^{\perp_1}$ est le sous-module de E de base $i - \beta_1(e,i)e$.

- D'autre part la multiplication définie sur le A-module E par la relation $XX' = - B_1(X,X')e + B_1(X,e)X' + B_1(X',e)X$ munit le module E d'une structure de N-algèbre d'unité e donc coïncide avec la multiplication de l'algèbre quadratique E.

Remarques.

- La propriété (1.2.10)' est une conséquence de la propriété (1.2.10)

- La proposition 1.2.11 reste vraie lorsqu'on remplace la propriété (1.2.10) par la propriété (1.2.10)' et $(Ae)^{\perp}$ par $(Ae)^{\perp_1}$ (la preuve est analogue à la précédente).

On note (1.2.11)' la proposition analogue à (1.2.11) relative à B_1.

CHAPITRE II

IDEAUX LIBRES DE RANG 2 D'UNE ALGEBRE QUADRATIQUE

---

§ 1 - *Structures d'idéal d'algèbre quadratique sur un A-module quadratique libre de rang 2.*

La norme d'une algèbre quadratique induit sur tout idéal libre de rang 2 de cette algèbre une structure de module quadratique libre de rang 2. On est amené à généraliser le problème 1 comme suit :

Problème 2.

Soit (E,Q) un A-module quadratique libre de rang 2.
Peut-on trouver un idéal E' d'une algèbre quadratique et un isomorphisme quadratique σ de (E,Q) sur (E',N) où N désigne la norme de l'algèbre ?

Lorsque E' et σ existent, E s'identifie par σ à un idéal d'une algèbre quadratique.

Avant d'étudier les solutions du problème 2, on établit deux résultats préliminaires.

1 - Etude des idéaux libres de rang 2 d'une algèbre quadratique.

Soit F une algèbre quadratique d'unité f, de base (f,j), de norme N. B_N désignant la forme bilinéaire associée à N. On pose $N(j) = -\alpha$, $B_N(f,j) = \beta$.

a) Condition nécessaire et suffisante pour qu'un sous-module libre de rang 2 de F soit un idéal de F.

Soit E un sous A-module de F, de base (e_1,e_2), $(e_1 = u_1 f + v_1 j$, $e_2 = u_2 f + v_2 j)$. Soit $\delta = u_1v_2 - u_2v_1$. Le déterminant δ est un élément régulier de A et si on choisit une autre base pour E, le déterminant associé est de la forme $\delta' = \delta u$ avec u inversible.

Pour que E soit un idéal de F, il faut et il suffit que fe_1, fe_2, je_1, je_2 appartiennent à E.

Comme $fe_1 = e_1$, $fe_2 = e_2$, $je_1 = u_1 f + v_1(\alpha f + \beta j)$, $je_2 = u_2 f + v_2(\alpha f + \beta j)$ cette condition équivaut à l'existence d'éléments x, y, x', y' de A tels que :

$$u_1 j + v_1(\alpha f + \beta j) = x\,(u_1 f + v_1 j) + y\,(u_2 f + v_2 j)$$

$$u_2 j + v_2(\alpha f + \beta j) = x'(u_1 f + v_1 j) + y'(u_2 f + v_2 j)$$

c'est-à-dire tels que :

$$u_1 x + u_2 y = \alpha v_1 \,,\; v_1 x + v_2 y = u_1 + \beta v_1$$

et $$u_1 x' + u_2 y' = \alpha v_2 \,,\; v_1 x' + v_2 y' = u_2 + \beta v_2$$

$u_1 v_2 - u_2 v_1$ est le déterminant δ de la base (e_1, e_2) de E.

Donc, pour que E soit un idéal de F, il faut et il suffit qu'il existe des éléments x, y, x', y' de A tels que :

$$\left.\begin{aligned}
&(1) \quad \delta x = -(u_1 u_2 - \alpha v_1 v_2 + \beta u_2 v_1) \\
&(2) \quad \delta y = u_1^2 + \beta u_1 v_1 - \alpha v_1^2 \\
&(3) \quad \delta x' = -u_2^2 - \beta u_2 v_2 + \alpha v_2^2 \\
&(4) \quad \delta y' = u_1 u_2 - \alpha v_1 v_2 + \beta u_1 v_2
\end{aligned}\right\} \quad (2.1.1.)$$

Lorsque 2 est régulier dans A, le système (2.1.1.) est équivalent au système (2.1.1.)'

$$\left.\begin{aligned}
&(1') \quad 2\delta x = \beta\delta - B_N(e_1, e_1) \\
&(2) \quad \delta y = N(e_1) \\
&(3) \quad \delta x' = -N(e_2) \\
&(4') \quad 2\delta y' = \beta\delta + B_N(e_1, e_2)
\end{aligned}\right\} \quad (2.1.1.)'$$

$(u_1^2+\beta u_1 v_1-\alpha v_1^2) = N(e_1)$, $u^2 + \beta u_2 v_2 - \alpha v_2^2 = N(e_2)$ et on vérifie aisément que $- 2(u_1u_2-\alpha v_1 v_2+ \beta u_2 v_1) = \beta\delta - B_N(e_1,e_2)$, $2(u_1,u_2-\alpha v_1 v_2+\beta u_1 v_2) = \beta\delta + B_N(e_1,e_2)$).

Pour que le système (2.1.1.)' admette une solution (x,y,x',y') il faut et il suffit que δ divise $N(e_1)$, $N(e_2)$ et $B_N(e_1,e_2)$, c'est-à-dire que δ divise la norme de tout élément de E.

Dans le cas général, pour que le système (2.1.1.) admette une solution (x,y,x',y'), il est nécessaire que δ soit un diviseur de la norme sur E. (En effet, ((1) et (4)) $\Rightarrow$ $\delta(y'-x) = B_N(e_1,e_2)$) .

b) Condition nécessaire et suffisante d'isomorphie quadratique de deux idéaux libres de rang 2 de l'algèbre quadratique F.

Soient E et E' deux sous A-modules de F libres de rang 2 et σ un isomorphisme de E sur E'. Soient (e_1,e_2) une base de E et (e'_1,e'_2) la base homologue, $(e'_1= \sigma(e_1), e'_2= \sigma(e_2))$. On désigne par δ , (resp. δ'), le déterminant relatif à (f,j) de (e_1,e_2), (resp. (e'_1,e'_2)).

On utilise une méthode d'extension de scalaires.

Soient S l'ensemble des éléments réguliers de A, $S^{-1}A$ l'anneau total de fractions de A et $S^{-1}F$ l'algèbre obtenue par extension des scalaires à $S^{-1}A$. On identifie A et F à leurs images respectives dans $S^{-1}A$ et $S^{-1}F$ par les injections canoniques. $S^{-1}F$ est alors une $S^{-1}A$ algèbre quadratique d'unité f, de base (f,j) telle que $j^2 = \alpha f + \beta j$. La norme sur F est la restriction à F de la norme N_o sur $S^{-1}F$. Les couples (e_1,e_2) et (e'_1,e'_2) ont des déterminants inversibles dans $S^{-1}A$ donc constituent des bases du $S^{-1}A$-module $S^{-1}F$. Tout isomorphisme de E sur E' se prolonge à un $S^{-1}A$-automorphisme du module $S^{-1}F$.

Proposition 2.1.2.

Soient F une algèbre quadratique d'unité f, de norme N, E et E'

deux sous A-modules libres de rang 2 de F, σ un isomorphisme de E sur E'. On désigne par $S^{-1}F$ l'algèbre quadratique obtenue par extension des scalaires à l'anneau total de fractions $S^{-1}A$ de A et on identifie A et F à leurs images respectives dans $S^{-1}A$ et $S^{-1}F$ par les injections canoniques.

Pour qu'il existe deux éléments réguliers k et k' de A tels que, pour tout élément X de E, $k'N(X) = kN(\sigma(X))$, il faut et il suffit que l'automorphisme σ_o de $S^{-1}F$ qui prolonge σ puisse être mis sous la forme $m_{f'} \circ \tau_o$ où $m_{f'}$ est la multiplication par un élément f' de $S^{-1}F$ de norme $k'k^{-1}$ et τ_o un automorphisme d'algèbre de $S^{-1}F$.

Preuve.

Si $k'N(X) = kN(\sigma(X))$ pour tout élément X de E, $k'N_o(y) = kN_o(\sigma_o(y))$ pour tout élément y de $S^{-1}F$. En particulier $N_o(\sigma_o(f)) = k'k^{-1}$. Soit $f' = \sigma_o(f)$. Puisque $k'k^{-1}$ est inversible dans $S^{-1}A$, f' est un élément inversible de $S^{-1}F$ (prop. 1.2.1., cor. 1). L'application $\tau_o = m_{f'^{-1}} \circ \sigma_o$ est une transformation orthogonale de $S^{-1}F$ qui conserve f, c'est donc un automorphisme d'algèbre de $S^{-1}F$ (prop. 1.1.2.) et $\sigma_o = m_{f'} \circ \tau_o$.

Inversement, lorsque $\sigma_o = m_{f'} \circ \tau_o$ où τ_o est un automorphisme d'algèbre de $S^{-1}F$ et $N(f') = k'k^{-1}$, on a, pour tout élément X de $S^{-1}F$, $N_o(\sigma_o(X)) = N_o(f')N_o(\tau_o(X)) = k'k^{-1}N_o(\tau_o(X)) = k'k^{-1}N_o(X)$ d'où, pour tout élément X de E, $k'N(X) = kN(\sigma(X))$.

La proposition 2.1.2. donne en particulier une condition nécessaire et suffisante pour que σ soit un isomorphisme quadratique de E sur E'. Il suffit de prendre $k = k'$.

Corollaire.

Les notations sont celles de la proposition 2.1.2. Soit E un sous A-module libre de rang 2 de l'algèbre quadratique F. Les sous-modules de F images de E par les isomorphismes de A-modules compatibles avec la norme sont les modules de F de la forme $f'E''$ où f' est un élément de norme 1 de

$S^{-1}F$ et E'' l'image de E par un automorphisme de l'algèbre $S^{-1}F$.

Cas particulier.

Lorsque A est intègre et lorsque $K = (0)$, (resp. $H = \{0\}$ et $K \neq (0)$), (not. 0.1.1.) il existe exactement deux automorphismes, (resp. un automorphisme), d'algèbre de $S^{-1}F$. Les restrictions à F de ces automorphismes sont les automorphismes de F. Dans ce cas, pour que l'isomorphisme σ de E sur E' soit compatible avec la norme, il faut et il suffit qu'on puisse le mettre sous la forme $\sigma_1 \circ \tau$, où τ est un automorphisme de l'algèbre F et σ_1 la restriction à $\tau(E)$ de la multiplication par f', élément de norme 1 de $S^{-1}F$.

La proposition 2.1.2. et le corollaire s'appliquent en particulier aux idéaux libres de rang 2 d'une algèbre quadratique.

2 - Etude du problème 2.

La forme norme munit toute algèbre quadratique et tout sous-module de cette algèbre d'une structure de module quadratique. Dans ce qui suit, lorsqu'on parle de structure de module quadratique d'une algèbre quadratique ou d'un sous-module de cette algèbre, il s'agit toujours de la structure définie par la norme.

a) Théorème d'existence. Caractérisation des solutions.

Théorème 2.1.3.-

Soit (E,Q) un A-module quadratique libre de rang 2. Pour qu'il existe une algèbre quadratique F de norme N, un idéal E' de cette algèbre et un isomorphisme quadratique σ de (E,Q) sur (E',N), (autrement dit, pour qu'il existe une solution du problème 2), il faut et il suffit qu'il existe δ, élément régulier de A, diviseur de $Q(X)$ pour tout $X \in E$, et $V \in E$ tels que $Q(V) = \delta^2$.

Une solution du problème 2 est formée d'une algèbre F de norme N, d'un idéal E' de F et d'un isomorphisme quadratique σ de (E,Q) sur (E',N). On peut convenir d'identifier deux solutions (F,E',σ) et (F_1,E'_1,σ_1) lorsqu'il existe

un isomorphisme τ de l'algèbre F sur l'algèbre F_1 tel que $\tau(E') = E'_1$, $\sigma_1 = \tau \circ \sigma$.

Avec cette convention, il existe une correspondance biunivoque entre les couples (V,δ) vérifiant la condition de ce théorème, définis à un facteur inversible près, et les solutions du problème 2.

(Les couples (V,δ) et $(tV, t\delta)$ où t est un élément inversible de A correspondent à la même solution).

Preuve.

On utilisera plusieurs lemmes.

Soit (E,Q) un A-module quadratique libre de rang 2. On cherche d'abord s'il existe une algèbre quadratique F, de norme N, un sous-module E' de F et un isomorphisme quadratique σ de (E,Q) sur (E',N). Lorsqu'on fixe une base (e_1,e_2) de E et lorsqu'on se donne un A-module F de base (f,j), cela revient à chercher un couple (α,β) d'éléments de A qui détermine une multiplication d'unité f sur F par la relation $j^2 = \alpha f + \beta j$ et une base $(\sigma(e_1), \sigma(e_2))$ du sous-module E'.

Le lemme 1 donne une condition d'existence et une caractérisation des solutions (F,E',σ) de ce problème préliminaire.

Lemme 1.-

1) Soit (E,Q) un A-module quadratique de base (e_1,e_2). Pour que (E,Q) puisse être identifié à un sous-module d'une algèbre quadratique par un isomorphisme quadratique, il faut et il suffit qu'il existe un couple (V,W) d'éléments de E, de déterminant δ régulier dans A et deux éléments α et β de A tels que $Q(V) = \delta^2$, $Q(W) = -\alpha\delta^2$, $B(V,W) = \beta\delta^2$. (B : forme bilinéaire associée à Q).

Lorsque cette condition est vérifiée, E peut être identifié à un

sous-module E' d'une algèbre F, d'unité f, de base (f,j) telle que $j^2 = \alpha f + \beta j$, par un isomorphisme quadratique σ tel que $\sigma(V) = \delta f$ et $\sigma(W) = \delta j$.

A une solution (F,E',σ) de ce problème préliminaire et à une base (f,j) de F correspond un couple unique (V,W) d'éléments de E tels que $\sigma(V) = \delta f$, $\sigma(W) = \delta j$ où δ est le déterminant de $(\sigma(e_1), \sigma(e_2))$ relatif à (f,j). (Lorsque $\sigma(e_1) = u_1 f + v_1 j$, $\sigma(e_2) = u_2 f + v_2 j$ $(u_1,u_2,v_1,v_2, \in A)$, $V = v_2 e_1 - v_1 e_2$, $W = - u_2 e_1 + u_1 e_2$).

Les solutions (F_1,E'_1,σ_1) où une base de F_1 contenant l'unité est fixée, auxquelles correspond le même couple (V,W) sont les triples de la forme $(\tau(F), \tau(E'), \tau \circ \sigma)$ où τ est un isomorphisme d'algèbres.

2) Soient (F,E',σ) une solution, (f,j) une base de F contenant l'unité f et (V,W) le couple associé de déterminant δ . Alors, l'ensemble des couples (V_1,W_1) associés aux différentes bases (f,j_1) de F est l'ensemble des couples (tV,W_1) de déterminant δ_1 tels que t soit un élément inversible de A, (tV,W_1) une base du sous-module $[V,W]$ de E et $\delta_1 = t\delta$.

Preuve du lemme 1.

On suppose qu'il existe une solution (F,E',σ) de ce problème préliminaire. F est une algèbre quadratique d'unité f, de base (f,j) telle que $j^2 = \alpha f + \beta j$, E' un sous-module de F de base (e'_1,e'_2) homologue de la base (e_1,e_2) de E. Lorsque $e'_1 = u_1 f + v_1 j$ et $e'_2 = u_2 f + v_2 j$, $\delta = u_1 v_2 - u_2 v_1$. Le déterminant δ est un élément régulier de A, δf et δj sont des éléments de E', $(\delta f = v_2 e'_1 - v_1 e'_2$, $\delta j = - u_2 e'_1 + u_1 e'_2)$. $N(\delta f) = \delta^2$, $N(\delta j) = - \alpha\delta^2$, $B_N(\delta f, \delta j) = \beta\delta^2$. Il existe donc un couple (V,W) d'éléments de E tels que $\sigma(V) = \delta f$, $\sigma(W) = \delta j$, $Q(W) = - \alpha\delta^2$ et $B(V,W) = \beta\delta^2$. Le couple (V,W) dépend du choix de la base (f,j) de F. Il est déterminé lorsque cette base est fixée et a pour déterminant δ relativement à (e_1,e_2). En effet $V = v_2 e_1 - v_1 e_2$, $W = - u_2 e_1 + u_1 e_2$.

Inversement soit (V,W) un couple d'éléments de E de déterminant régulier et α et β vérifiant les conditions indiquées. Soient u_1,u_2,v_1,v_2 tels que $V = v_2e_1 - v_1e_2$, $W = -u_2e_1 + u_1e_2$ et soit $\delta = u_1v_2 - u_2v_1$. On considère une algèbre quadratique F d'unité f, de base (f,j) telle que $j^2 = \alpha f + \beta j$ et le sous-module E' de F engendré par $e'_1 = u_1f + v_1j$, $e'_2 = u_2f + v_2j$. Puisque δ est régulier, E' est libre de rang 2. Alors (F,E',σ) où σ est défini par $\sigma(e_1) = e'_1$, $\sigma(e_2) = e'_2$ est une solution du problème préliminaire.

En effet :

$\delta e_1 = u_1V + v_1W$, $\delta e_2 = u_2V + v_2W$, $N(j) = -\alpha$, $B_N(f,j) = \beta$ donc $Q(\delta e_1) = u_1^2\,Q(V) + u_1v_1\,B(V_1,W_1) + v_1^2\,Q(W) = \delta^2(u_1^2 + \beta u_1v_1 - \alpha v_1^2) = \delta^2\,N(e'_1)$ et puisque δ est régulier, $Q(e_1) = N(e'_1)$. De même $Q(e_2) = N(e'_2)$, $B(e_1,e_2) = B_N(e'_1,e'_2)$.

La fin de la partie 1 du lemme est immédiate puisque la donnée du couple (V,W) détermine δ, α, β et la base de E'.

2) Soient (F,E',σ) une solution, (f,j) une base de F contenant l'unité f et (V,W) le couple associé, $(V = v_2e_1 - v_1e_2,\ W = -u_2e_1 + u_1e_2)$ Soit (f,j_1) une autre base de F, $j = sf + tj_1$ $(s,\ t \in A,\ t$ inversible$)$. $\sigma(e_1) = u_1f + v_1j = (u_1+sv_1)f + tv_1j_1$, $\sigma(e_2) = u_2f + v_2j = (u_2+sv_2)f + tv_2j_1$. Le couple (V_1,W_1) associé à (F,E',σ) et à la base (f,j_1) est donné par $V_1 = tv_2e_1 - tv_1e_2 = tV$, $W_1 = -(u_2+sv_2)\,e_1 + (u_1+sv_1)\,e_2 = -sV + W$. On en déduit que $V_1 = tV$, que (V_1,W_1) est une base du sous-module $[V,W]$ de E et que le déterminant de (V_1,W_1) relatif à (e_1,e_2) est $t\delta$.

Inversement, soit (V_1,W_1) un couple d'éléments de E de déterminant $t'\delta$ avec t' inversible tel que $V_1 = t'V$ et tel que (V_1,W_1) soit une base du sous-module $[V,W]$ de E. W_1 est alors de la forme $s'V + W$, $(s' \in A)$. Il est immédiat qu'il est associé à la solution (F,E',σ) et à la base (f,j'_1) de F définie par $j = s'f + t'j'_1$.

Le lemme suivant est une conséquence immédiate du lemme 1 et de l'étude (1,a) de ce paragraphe § 1.

Lemme 2.-

Soit (E,Q) un A-module quadratique de base (e_1,e_2). Pour qu'il existe un isomorphisme quadratique de (E,Q) sur un idéal d'une algèbre quadratique, il faut et il suffit qu'il existe un couple $(V = v_2e_1 - v_1e_2,\ W = -u_2e_1 + u_1e_2)$, $(u_1,u_2,v_1,v_2 \in A)$, de déterminant δ régulier, vérifiant les conditions suivantes :

1) $Q(V) = \delta^2$ et il existe α et $\beta \in A$ tels que $Q(W) = -\alpha\delta^2$, $B(V,W) = \beta\delta^2$

2) Le système (2.1.1.) du (1,a) admet une solution (x,y,x',y') formée d'éléments de A.

En effet, la condition 1 est une condition nécessaire et suffisante d'existence d'un isomorphisme quadratique de (E,Q) sur un sous-module E' d'une algèbre quadratique (lemme 1). La condition 2 est la condition nécessaire et suffisante pour que ce sous-module E' soit un idéal de l'algèbre quadratique (Etude (1,a) du §1).

D'après l'étude (1,a) pour que le système (2.1.1.) admette une solution (x,y,x',y') il faut que δ divise $N(X')$ pour tout élément X' de E', c'est-à-dire que δ divise $Q(X)$ pour tout élément X de E.

On pose $Q(e_1) = a$, $Q(e_2) = c$, $B(e_1,e_2) = b$. Les deux lemmes suivants permettront d'associer les solutions du problème 2 aux couples (V,δ) définis à un facteur inversible près tels que δ divise a,b,c et tels que $Q(V) = \delta^2$.

Lemme 3.-

Soit (E,Q) un A-module quadratique de base (e_1,e_2). On pose $Q(e_1) = a$, $Q(e_2) = c$, $B(e_1,e_2) = b$. Soit δ un diviseur commun à a,b,c. S'il existe $V \in E$ tel que $Q(V) = \delta^2$, il existe $W \in E$ tel que le couple (V,W) ait pour déterminant δ et vérifie les conditions du lemme 2.

Preuve du lemme 3.

Soit $V = me_1 + ne_2$ tel que $Q(V) = \delta^2$. On pose $W = -c'ne_1 + (a'm+b'n)e_2$, a',b',c' désignant les quotients respectifs de a,b,c par δ. Compte tenu de l'égalité $Q(V) = \delta^2$, $m(a'm+b'n) + nc'n = \delta$, $Q(W) = a'c'\delta^2$, $B(V,W) = b'\delta^2$. Donc le couple (V,W) vérifie la condition 1 du lemme 2 pour $\alpha = -a'c'$, $\beta = b'$. Pour reprendre les notations précédentes, on pose $m = v_2$, $n = -v_1$.

Lorsque 2 est régulier, le système (2.1.1.) du (1,a) est équivalent au système (2.1.1.)' qui s'écrit ici :

$$2\delta x = \beta\delta - b$$

$$\delta y = a$$

$$\delta x' = -c$$

$$2\delta y = \beta\delta + b$$

et qui admet la solution évidente (o,a',-c',b').

Lorsque 2 n'est pas régulier, on vérifie directement que (o,a',-c',b') est encore une solution de (2.1.1.).

Lemme 4.-

Soit (E,Q) un A-module quadratique de base (e_1,e_2) telle que $Q(e_1) = a$, $Q(e_2) = c$, $B(e_1,e_2) = b$. On suppose qu'il existe δ élément régulier de A diviseur commun à a,b,c et $V \in E$ tels que $Q(V) = \delta^2$. Si deux couples (V,W) et (V,W') de déterminant δ vérifient les conditions du lemme 2, (V ,W') est une base du sous-module $[V,W]$ de E et par suite les solutions associées à (V,W) et (V,W') coïncident.

Preuve.

Soient $V = v_2e_1 - v_1e_2$, $W = -u_2e_1 + u_1e_2$, $W' = -u'_2e_1 + u'_1e_2$.
Puisque $\delta e_1 = u_1V + v_1W$ et $\delta e_2 = u_2V + v_2W$, $\delta W' = (-u'_2u_1+u'_1u_2)\ V + \delta W$. Pour que (V,W') soit une base du module $[V,W]$, il faut et il suffit que δ divise $-u'_2u_1 + u'_1u_2$.

Il suffit de prouver le lemme lorsque W est l'élément de E utilisé dans le lemme 3. Alors $u_2 = -c'v_1$, $u_1 = a'v_2 - b'v_1$ et $-u'_2u_1 + u'_1u_2 = -a'u'_2v_2 + b'u'_2v_1 - c'u'_1v_1$.

Puisque W' vérifie les conditions du lemme 2 relativement à V et δ, on obtient, pour $\alpha' = -\frac{Q(W')}{\delta^2}$ et $\beta' = \frac{B(V,W')}{\delta^2}$, $a = u_1'^2 + \beta'u'_1v_1 - \alpha' v_1^2$, $c = u_2'^2 + \beta' u'_2v_2 - \alpha'v_2^2$, $b = 2u'_1u'_2 - 2\alpha'v_1v_2 + \beta'(u'_1v_2+u'_2v_1)$. En reportant ces valeurs dans $-a'u'_2v_2 + b'u'_2v_1 - c'u'_1v_1$ on obtient

$$- a'u'_2v_2 + b'u'_2v_1 - c'u'_1v_1 = - u'_1u'_2 + \alpha'v_1v_2 - \beta'u'_2v_2$$

Or, le second membre de cette dernière équation est le second membre de l'équation (1) du système (2.1.1.) pour les coefficients $v_1, v_2, u'_1, u'_2, \alpha', \beta'$ relatifs à V et W'. Donc δ divise $-u'_2u_1 + u'_1u_2$ et (V,W') est une base du A-module $[V,W]$. On sait que dans ce cas les solutions associées à (V,W) et (V,W') sont les mêmes (partie 2 du lemme 1).

On peut maintenant terminer la preuve du théorème 2.1.3.

A toute solution (F,E',σ) correspond une famille de couples (V,δ) vérifiant les conditions du théorème. Si (V,δ) est l'un de ces couples, les autres couples sont les couples $(tV,t\delta)$ où t décrit l'ensemble des éléments inversibles de A.

En effet, à une solution (F,E',σ) et à une base de F correspond un couple (V,W) d'éléments de E de déterminant δ vérifiant les conditions du lemme 2, donc le couple (V,δ) vérifie les conditions du théorème. Pour tout élément inversible t de A, le couple (tV,W) a pour déterminant $t\delta$ et forme une base du module $[V,W]$. D'après le lemme 1, il est aussi associé à (F,E',σ) ainsi que le couple $(tV,t\delta)$ correspondant. Inversement tout couple d'éléments de E associé à $(F,E',\ )$ est de la forme (tV,W_1) où t est inversible, et a pour déterminant $t\delta$ (lemme 1). Il lui correspond $(tV,t\delta)$.

Inversement, soit (V,δ) un couple dans lequel δ est un élément régulier de A diviseur de $Q(X)$ pour tout élément X de E et tel que $Q(V) = \delta^2$. D'après les lemmes 3 et 4, il correspond à ce couple une famille de couples (V,W) d'éléments de E tels que les conditions du lemme 2 soient vérifiées et les solutions associées à deux quelconques de ces couples sont les mêmes.

Si de plus on convient d'identifier deux solutions (F,E',σ) et (F_1,E'_1,σ_1) lorsqu'il existe un isomorphisme d'algèbres τ de F sur F_1 tel que $E'_1 = \tau(E')$ et $\sigma_1 = \tau \circ \sigma$, alors au couple (V,δ) correspond une solution unique du problème 2 (partie 1 du lemme 1). On désignera une solution du problème 2 par l'un des triples (F,E',σ) qui la définissent.

Remarque.

La solution associée à un couple (V,δ) vérifiant les hypothèses du théorème 2.1.3. est la solution associée en particulier au couple (V,W) d'éléments de E où W est l'élément utilisé dans la preuve du lemme 3, (si $V = me_1 + ne_2$, $W = -c'ne_1 + (a'm+b'n)\,e_2$). Pour ce choix, $\alpha = -\frac{Q(W)}{\delta^2} = -a'c'$, $\beta = \frac{B(V,W)}{\delta^2} = b'$. Dans la suite, sauf précision contraire, les couples utilisés seront de ce type.

b) Etude des solutions du problème 2.

1°) Solutions correspondant à un diviseur δ fixé

Proposition 2.1.4.-

Soit (E,Q) un A-module quadratique de base (e_1,e_2) telle que $Q(e_1) = a$, $Q(e_2) = c$, $B(e_1,e_2) = b$ et soit δ un élément régulier de A diviseur commun à a,b,c. On suppose qu'il existe deux éléments V et V_1 de E tels que $Q(V) = Q(V_1) = \delta^2$ et on désigne par W et W_1 les éléments associés à V et V_1 selon la remarque du théorème 2.1.3.

Deux cas peuvent se présenter.

1) Il existe une transformation orthogonale ϕ de E telle que

$\phi(V) = V_1$, et $\phi(W) = W_1$. Alors, à (V,δ) et (V_1,δ) correspondent respectivement les solutions (F,E',σ) et (F,E',σ_1) où $\sigma = \sigma_1 \circ \phi$.

2) Une telle transformation n'existe pas. Alors, à (V,δ) et (V_1,δ) correspondent respectivement les solutions (F,E',σ) et (F,E'_1,σ_1) où **E'** et E'_1 sont deux idéaux distincts d'une même algèbre F.

Preuve.

Soient $V = me_1 + ne_2$, $V_1 = m_1e_1 + n_1e_2$, vérifiant les hypothèses ci-dessus. On pose $p = -c'n$, $q = a'm + b'n$, $p_1 = -c'n_1$, $q_1 = a'm_1 + b'n_1$ $(a',b',c'$ sont les quotients respectifs de a,b,c par $\delta)$. Soient $W = pe_1 + qe_2$, $W_1 = p_1e_1 + q_1e_2$. Aux couples (V,W) et (V_1,W_1) est associée une algèbre de base (f,j) telle que $j^2 = -a'c'f + b'j$.

On suppose qu'il existe une transformation orthogonale ϕ de E telle que $\phi(V) = V_1$ et $\phi(W) = W_1$. Soit $(F'E'_1,\sigma_1)$ associée à (V_1,W_1), alors $\sigma_1 \circ \phi$ est un isomorphisme quadratique de E sur E'_1 et $(\sigma_1 o\phi)(V) = \sigma_1(V_1) = \delta f$, $(\sigma_1 o\phi)(W) = \sigma_1(W_1) = \delta j$. Donc $(F,E'_1,\sigma_1 o\phi)$ est un triple associé à (V,W) (lemme 1). L'ensemble des triples associés à (V_1,δ) est l'ensemble des triples $(\tau(F), \tau(E'_1), \tau \circ \sigma_1)$ où τ est un isomorphisme d'algèbres, l'ensemble des triples associés à (V,δ) est l'ensemble des triples $(\tau(F), \tau(E'_1), (\tau o\ \sigma_1)\ o\phi)$.

Inversement, lorsqu'on peut associer aux couples (V,δ) et (V_1,δ) les triples (F,E',σ) et (F,E',σ_1) avec le même idéal E', $\sigma_1^{-1} \circ \sigma$ est une transformation orthogonale de E telle que $(\sigma_1^{-1} \circ \sigma)(V) = \sigma_1^{-1}(\delta f) = V_1$, $(\sigma_1^{-1} \circ \sigma)(W) = \sigma_1^{-1}(\delta j) = W_1$ et $\sigma = \sigma_1 o(\sigma_1^{-1} \circ \sigma)$.

Donc lorsqu'il n'existe aucune transformation orthogonale ϕ de E telle que $\phi(V) = V_1$ et $\phi(W) = W_1$, aux couples (V,W) et (V_1,W_1) sont associées les triples (F,E',σ) et (F,E'_1,σ_1) où E' et E'_1 sont des idéaux distincts d'une même algèbre. L'ensemble des triples associés à (V,δ) est l'ensemble des triples $(\tau(F), \tau(E'), \tau \circ \sigma)$, l'ensemble associé à (V_1,δ) est l'en-

semble des triples $(\tau(F), \tau(E_1'), \tau \circ \sigma_1)$ et on n'a jamais $\tau(E) = \tau(E_1')$.

Le cas 2 peut effectivement se présenter. En effet :

Pour qu'il existe une transformation orthogonale ϕ de E telle que $\phi(V) = V_1$, $\phi(W) = W_1$, il faut qu'il existe une matrice T_ϕ telle que, avec les notations du début de la preuve,

$$T_\phi = \begin{pmatrix} r & r' \\ s & s' \end{pmatrix}$$

$$mr + nr' = m_1 \qquad pr + qr' = p_1$$
$$ms + ns' = n_1 \qquad ps + qs' = q_1$$

c'est-à-dire telle que le système suivant admette une solution (r,s,r',s') formée d'éléments de A.

$$\delta r = qm_1 - np_1 = a'mm_1 + b'nm_1 + c'nn_1$$
$$\delta r' = -pm_1 + mp_1 = c'(nm_1 - mn_1)$$
$$\delta s = qn_1 - q_1 n = a'(mn_1 - nm_1)$$
$$\delta s' = -pn_1 + mq_1 = a'mm_1 + b'n_1 m + c'nn_1$$

Pour que ϕ existe, il faut donc que δ divise les seconds membres. Mais δ ne divise pas nécessairement les seconds membres.

Exemple.

$A = \mathbb{Z}$ $a = -15$ $b = -3 \times 15$ $c = 19 \times 15$

$V = e_1 + e_2$ $V_1 = -4e_1 + e_2$. Alors $Q(V) = Q(V_1) = (-15)^2$ mais -15 ne divise pas $a'(mn_1 - nm_1)$ qui est égal à 5.

Donc le deuxième cas peut se présenter.

Les idéaux E' et E_1' sont homologues dans un isomorphisme quadratique. Ces isomorphismes ont été étudiés dans la partie (1,b) de ce paragraphe (prop. 2.1.2.). On peut voir ici que l'idéal E_1' associé à V_1, de base

$(-f-j, -19f-4j)$, est déduit de l'idéal E' associé à V, de base $(4f-j,-19f+j)$, par la multiplication par $\frac{4}{3} f + \frac{1}{3} j$ dans l'algèbre $S^{-1} F$ (notations de la proposition 2.1.2.).

Remarques.

- Pour toute solution (F,E',σ) du problème 2 et toute transformation orthogonale ϕ de E, $(F,E',\sigma o\phi)$ est encore une solution.

- On retrouve les résultats du chapitre (I) lorsque $\delta = 1$.

2°) Etude des solutions associées à différents diviseurs communs à a,b,c

On envisage le cas particulier de deux diviseurs d et δ tels que δ divise d.

Proposition 2.1.5.-

Soient (E,Q) un A-module quadratique de base (e_1,e_2) telle que $Q(e_1) = a$, $Q(e_2) = c$, $B(e_1,e_2) = b$ et d et δ deux éléments réguliers de A diviseurs communs à a,b,c tels que δ divise d. On suppose qu'il existe un élément V_δ de E tel que $Q(V_\delta) = \delta^2$. On pose $k = \frac{d}{\delta}$ et $V_d = k\, V_\delta$. Alors le couple (V_d,d) vérifie les conditions du théorème 2.1.3.

Soient (F_d,E'_d,σ_d) la solution associée à (V_d,d), W_d l'élément de E associé à V_d selon la remarque du théorème 2.1.3, et (f_d,j_d) la base de F_d associée à (V_d,W_d). Alors la sous-algèbre F_δ et F_δ, de base (f_d,kj_d) forme avec E'_d et σ_d la solution associée à (V_δ,δ).

Preuve.

Puisque $Q(V_\delta) = \delta^2$, $Q(V_d) = k^2\delta^2 = d^2$ et le couple (V_d,d) vérifie les conditions du théorème 2.1.3. Comparons les solutions associées à (V_δ,δ) et (V_d,d).

Soient $V_\delta = me_1 + ne_2$, a',b',c' les quotients respectifs de a,b,c par δ et a'',b'',c'' les quotients respectifs de a,b,c par d. Alors,

$W_\delta = -c'ne_1 + (a'm+b'n)e_1$, $W_d = -c''kne_1 + (a''km+b''km)e_2 = W_\delta$.

Soit (F_d,E'_d,σ_d) un triple solution associé à (V_d,d). F_d admet la base (f_d,j_d) correspondant à (V_d,W_d) où f_d est l'unité de F_d et $j_d^2 = -a''c''f_d + b''j_d$. De façon générale, lorsqu'un couple $(V = v_2e_1 - v_1e_2$, $W = -u_2e_1 + u_1e_2)$ est associé à une solution (F,E',σ) où (f,j) est la base de F, E' a pour base $(\sigma(e_1) = u_1f + v_1j, \sigma(e_2) = u_2f + v_2j)$, (lemme 1). Donc l'idéal E'_d a pour base $(qf_d - nkj_d, -pf_d + mkj_d)$. Alors la sous-algèbre F_δ de F_d, de base (f_d,kj_d) forme avec E'_d et σ_d un triple solution associé au couple (V_δ,δ).

En effet, on a bien $(kj_d)^2 = -a'c'f_d + b'(kj_d)$ et la base $\left(\sigma_d(e_1) = qf_d - n(kj_d), \sigma_d(e_2) = -pf_d + m(kj_d)\right)$ de E'_d est bien la base associée à (V_δ, W_δ).

Remarques.

- Lorsque k est inversible, les algèbres F_d et F_δ sont confondues ainsi que (F_d,E'_d,σ_d) et $(F_\delta,E'_\delta,\sigma_\delta)$. Ce résultat a déjà été établi (lemme 1).

- Lorsque k n'est pas inversible, les algèbres F_d et F_δ ne sont pas isomorphes mais induisent la même multiplication sur E'_d. Lorsqu'on identifie E à E'_d par σ_d, on munit E à la fois d'une structure d'idéal de F_d et d'une structure d'idéal de F_δ.

La proposition 2.1.5. permet de ramener la recherche des solutions à la recherche des solutions associées au p.g.c.d de a,b,c lorsque A est un anneau factoriel. En effet :

Soit d le p.g.c.d de a,b,c. Tout diviseur δ de a,b,c divise d. A chaque solution $(F_\delta,E',\sigma_\delta)$ on peut associer une solution (F_d,E',σ_d) relative à d telle que F_δ soit une sous algèbre de F_d, E' un idéal commun aux deux algèbres et telle que $\sigma_d = \sigma_\delta$. Inversement, si (F_d,E',σ_d) est une solution relative à $d = k\delta$, on peut lui associer de la façon précédente une solution

relative à δ, à condition que (F_d,E',σ_d) soit associée à un élément V_d de E de la forme kV où V appartient à E. On obtient ainsi toutes les solutions relatives à δ.

§ 2 - *Correspondances entre classes d'idéaux et classes de formes quadratiques binaires.*

Définition 2.2.1.-

On considère l'ensemble des formes quadratiques binaires à coefficients dans A. (Chaque forme est caractérisée par la donnée de trois coefficients a,b,c appartenant à A. Sur cet ensemble, la relation binaire R définie par

$Q\ R\ Q' \iff$ (Q et Q' définissent la même forme quadratique sur un A-module libre de rang 2)

est une relation d'équivalence. Autrement dit, Q et Q' sont équivalentes selon R lorsqu'il existe un A-module E et deux bases (e_1,e_2), (e'_1,e'_2) de ce module telles que pour tout couple $((x,y),(x',y'))$ d'éléments de A^2 tel que $xe_1 + ye_2 = x'e'_1 + y'e'_2$, $Q(x,y) = Q'(x',y')$.

Soit σ l'automorphisme de E défini par $\sigma(e_1) = e'_1$, $\sigma(e_2) = e'_2$, on dit que Q' est équivalente à Q par l'intermédiaire de σ.

Dans le chapitre I et dans le paragraphe § 1 de ce chapitre II on a identifié les formes quadratiques binaires selon cette relation en parlant de forme quadratique définie sur un module libre de rang 2. Ici on ne fait pas cette identification. Pour distinguer ces deux notions on appellera forme quadratique une forme quadratique au sens du chapitre I et forme quadratique binaire un élément d'une classe d'équivalence selon R.

Première correspondance.

On utilisera les notations suivantes :

Notations 2.2.2.

On désigne par Φ le sous-ensemble de l'ensemble des formes quadratiques binaires à coefficients dans A caractérisé par la propriété suivante :

Pour tout $Q \in \Phi$, il existe d, élément régulier de A, et des éléments a_1, b_1, c_1 de A tels que :

1) $Q(x,y) = ax^2 + bxy + cy^2 = d(a_1x^2+2b_1xy+c_1y^2)$, $\forall (x,y) \in A^2$

2) Il existe $(m,n) \in A^2$ tel que $Q(m,n) = d^2$

A chaque élément α de A on fait correspondre le sous-ensemble Φ_α de Φ formé des éléments de Φ pour lesquels $b_1^2 - a_1 c_1 = \alpha$ pour un d convenable, et une algèbre quadratique F_α, d'unité f_α, de base (f_α, j_α) telle que $j_\alpha^2 = \alpha f_\alpha$. On désigne par N_α la norme de F_α et par $S^{-1}F_\alpha$ l'algèbre obtenue par extension des scalaires à l'anneau total de fractions $S^{-1}A$ de A (notations de la proposition 2.1.2.).

La relation R (déf. 2.2.1.) induit une relation d'équivalence sur Φ_α que l'on note encore R.

Proposition 2.2.3.-

Les notations sont les notations ci-dessus. Soit $\alpha \in A$.

On considère sur l'ensemble I_α des idéaux de F_α qui sont libres de rang 2 la relation d'équivalence T_α définie comme suit :

$E' \; T_\alpha \; E'' \iff$ (E'' est homologue de E' dans une transformation orthogonale de l'algèbre $S^{-1}F_\alpha$).

Alors, il existe une bijection de l'ensemble Φ_α/R sur l'ensemble I_α/T_α.

Preuve.

Soit $Q \in \Phi_\alpha$ et soit $(E,\bar{Q})$ un A-module quadratique de base (e_1,e_2) où $\bar{Q}$ est définie par $\bar{Q}(xe_1+ye_2) = Q(x,y)$, $\forall (x,y) \in A^2$. Par hypothèse, il existe

un élément régulier d de A, des éléments a_1, b_1, c_1 de A tels que $\frac{\bar{Q}(e_1)}{d} = a_1$, $\frac{\bar{Q}(e_2)}{d} = c_1$, $\frac{\bar{B}(e_1,e_2)}{d} = 2b_1$ et $b_1^2 - a_1 c_1 = \alpha$, et $(m,n) \in A^2$ tel que $d^2 = Q(m,n) = \bar{Q}(me_1+ne_2)$.

Soit $V = me_1 + ne_2$, alors le couple (V,d) vérifie les hypothèses du théorème 2.1.3. L'algèbre F_α est l'algèbre d'un triple solution du problème 2 associé à (V,d). En effet, puisqu'elle admet la base (f_α, j_α) où f_α est l'unité $j_\alpha^2 = \alpha f_\alpha$ et $\alpha = b_1^2 - a_1 c_1$, elle admet aussi la base (f_α, j') où $j' = b_1 f_\alpha - j_\alpha$ et $j' = -a_1 c_1 f_\alpha + 2b_1 j_\alpha$, qui est la base associée au couple (V,W) (remarque du théorème 2.1.3.). Il existe donc un idéal E' de F_α possédant une base (e_1', e_2') telle que pour tout élément (x,y) de A^2, $Q(x,y) = \bar{Q}(xe_1 + ye_2) = N_\alpha(xe_1' + ye_2')$.

Les idéaux de F_α qui vérifient cette propriété sont les idéaux homologues de E' dans une transformation orthogonale de l'algèbre $S^{-1} F_\alpha$ (prop.2.1.2.).

Inversement, soit E' un idéal de F_α libre de rang 2. La norme N_α induit une forme quadratique sur E' à laquelle correspond une forme quadratique binaire appartenant à Φ_α dès qu'une base est fixée. En effet, pour toute base (e_1', e_2') de E', le déterminant δ de (e_1', e_2') relatif à (f_α, j_α) divise $N_\alpha(xe_1' + ye_2')$, $\forall (x,y) \in A^2$. Avec les notations du système 2.1.1. ($e_1' = u_1 f_\alpha + v_1 j_\alpha$, $e_2' = u_2 f_\alpha + v_2 j_\alpha$), δ divise $u_1 u_2 - \alpha v_1 v_2$ puisque $\beta = o$. Comme $B_{N_\alpha}(e_1', e_2') = 2(u_1 u_2 - \alpha v_1 v_2)$, $\frac{B_{N_\alpha}(e_1', e_2')}{\delta}$ est un multiple de 2. De plus $v_2 e_1' - v_1 e_2' = \delta f_\alpha$, $N_\alpha(v_2 e_1' - v_1 e_2') = \delta^2$. Donc la forme Q définie par $Q(x,y) = N_\alpha(xe_1' + ye_2')$, $\forall (x,y) \in A^2$ appartient à Φ_α.

Les formes quadratiques binaires associées à deux bases de E' sont équivalentes selon R.

Il existe donc une bijection de Φ_α / R sur I_α / T_α.

Deuxième correspondance.

A chaque élément α de A on associe l'ensemble Φ_α^1 des formes

quadratiques binaires de la forme $a_1x^2 + 2b_1xy + c_1y^2$ qui représentent au moins un élément régulier de A et telles que $b_1^2 - a_1c_1 = \alpha$, et l'algèbre F_α précédente (notations 2.2.2.).

Soit $Q_1 \in \Phi_\alpha^1$. A chaque élément régulier d de A représente par Q_1, on fait correspondre la forme dQ_1 et les idéaux E de F_α possédant une base (e_1,e_2) de déterminant d telle que pour tout couple (x,y) d'éléments de A, $N_\alpha(xe_1+ye_2) = dQ_1(x,y)$. Il existe au moins un tel idéal E car la forme dQ_1 est un élément de Φ_α (correspondance précédente).

Soit E l'un de ces idéaux. Un idéal E' de F_α est associé à Q_1 par l'intermédiaire de la forme $d'Q_1$ si et seulement si il existe une base (e_1',e_2') de E' de déterminant d' telle que,

$$\forall (x,y) \in A^2,\ d'N_\alpha(xe_1 + ye_2) = d'dQ_1(x,y) = dN_\alpha(xe_1' + ye_2').$$

Soit σ l'automorphisme de E sur E' défini par $\sigma(e_1) = e_1'$, $\sigma(e_2) = e_2'$. D'après la proposition 2.1.2., l'automorphisme σ_o de $S^{-1}F_\alpha$ qui prolonge σ peut être mis sous la forme $m_{f'} \circ \tau_o$ où $m_{f'}$ est la multiplication par un élément f' de $S^{-1}F_\alpha$ de norme $d'd^{-1}$ et τ_o un automorphisme de l'algèbre $S^{-1}F_\alpha$. Cet automorphisme a pour déterminant 1 car le déterminant de $m_{f'} \circ \tau_o$ est égal à $d'd^{-1}$. Lorsque 2 est régulier ou lorsque l'anneau A est intègre τ_o est l'identité comme le montre immédiatement l'étude du système (1.2.7.) du (I, §2, 3) p. 18 lorsque $\beta = o$.

Inversement, soit E un idéal de F_α libre de rang 2. Une base (e_1,e_2) de E étant choisie, on lui associe une forme Q appartenant à Φ_α selon la correspondance précédente et la forme $Q_1 = Q/d$ où d désigne le déterminant de (e_1,e_2). Il est immédiat que Q_1 appartient à Φ_α^1. Lorsqu'on choisit une autre base (e_1',e_2') de déterminant d', on obtient une forme Q' équivalente à Q selon R et la forme Q_1'/d' associée. On étudie la relation entre Q_1 et Q_1'. Q' est la forme équivalente à Q obtenue par l'intermédiaire de l'automorphisme σ de E défini par $\sigma(e_1) = e_1'$, $\sigma(e_2) = e_2'$ (notations 2.2.1). Le déterminant

u de σ est inversible, $d' = du$ donc $uQ'_1 = Q'/d$ et la forme uQ'_1 est la forme équivalente à Q_1 obtenue par l'intermédiaire de σ.

Théorème 2.2.4.-

On garde les notations 2.2.2. Soit α un élément de A.

On considère sur l'ensemble I_α des idéaux de F_α qui sont libres de rang 2 la relation binaire T_1 définie comme suit :

$E\ T_1\ E' \iff$ (E' est homologue de E dans un isomorphisme σ dont l'extension à $S^{-1}F_\alpha$ est de la forme $m_{f'} \circ \tau_o$ où $m_{f'}$ est la multiplication par un élément de $S^{-1}F_\alpha$ et τ_o un automorphisme de l'algèbre $S^{-1}F_\alpha$ de déterminant 1).

De même on considère sur l'ensemble Φ^1_α des formes quadratiques binaires $a_1x^2 + 2b_1xy + c_1y^2$ telles que $b_1^2 - a_1c_1 = \alpha$ et qui représentent au moins un élément régulier de A la relation binaire R_1 définie comme suit :

$Q_1\ R_1\ Q'_1 \iff$ (il existe un élément inversible u de A tel que uQ'_1 soit la forme équivalente à Q_1 selon R obtenue par l'intermédiaire d'un automorphisme de détermiant u, (déf. 2.2.1.)).

Alors T_1 et R_1 sont des relations d'équivalence et il existe une bijection de I_α/T_1 sur Φ^1_α/R_1.

Il est facile de vérifier que T_1 et R_1 sont des relations d'équivalence. Le théorème résulte alors de l'étude précédente.

Remarque.

Lorsque 2 est régulier ou lorsque A est intègre, T_1 est définie par

$$E\ T\ E' \iff (\exists\ f' \mid f' \in S^{-1}F_\alpha \text{ et } E' = f'E)$$

En effet dans ce cas τ_o est l'identité sur S^{-1} [illegible].

Cas particuliers.

a) On suppose que A est un anneau principal.

Le produit de deux idéaux libres de rang 2 de F_α est un idéal libre de rang 2 (corollaire de la proposition 1.2.6). Puisque A est intègre, la relation T_1 est définie comme dans la remarque du théorème 2.2.4. et est donc compatible avec la multiplication des idéaux. On peut alors munir l'ensemble Φ_α^1/R_1 d'une structure de monoïde par l'intermédiaire de la bijection du théorème 2.2.4.

b) On suppose que A est principal, que 2 est inversible dans A et que α est sans facteurs carrés.

La norme N_α ne s'annule pas sur $F_\alpha - \{o\}$ donc F_α est intègre et $S^{-1} F_\alpha$ est le corps des fractions de F_α (prop. 1.2.1. cor. 3). De plus F_α est intégralement clos. En effet :

Pour qu'un élément X_o de $S^{-1} F_\alpha$ soit entier sur F_α, il faut et il suffit que sa norme $N_o(X_o)$ et sa trace $B_{N_o}(X_o, f_\alpha)$ dans $S^{-1} F_\alpha$ soient entières sur A (B.A.C. chap. V), c'est-à-dire, puisque A est intégralement clos, que $N_o(X_o)$ et $B_{N_o}(X_o, f_\alpha)$ soient des éléments de A. Donc, pour que F_α soit intégralement clos, il faut et il suffit que

$$(x \in S^{-1} A,\ y \in S^{-1} A,\ x^2 - \alpha y^2 \in A,\ 2x \in A) \Rightarrow (x \in A \text{ et } y \in A)$$

Puisque α est sans facteurs carrés et puisque 2 est inversible cette condition est vérifiée. F_α est alors un anneau de Dedekind (B.A.C. ch. VII § 2).

Puisque N_α ne s'annule pas sur F_α, I_α est l'ensemble des idéaux non nuls de F_α (prop. 1.2.8. et étude p. 16) et puisque A est intègre, la relation T_1 a la forme simplifiée de la remarque du théorème 2.2.4. L'ensemble I_α/T_1 peut alors être identifié au groupe des classes d'idéaux fractionnaires de F_α modulo le groupe des idéaux principaux et l'ensemble Φ_α^1/R_1 est muni d'une structure de groupe par l'intermédiaire de la bijection précédente.

c) On suppose que $A = \mathbb{Z}$, que $\alpha \equiv 2$ ou $3 \mod 4$ et que α est sans facteurs carrés.

F_α s'identifie alors à l'anneau des entiers du corps $Q(\sqrt{\alpha})$. La correspondance entre classes d'idéaux de F_α et classes de formes quadratiques binaires de discriminant 4α donnée par le théorème 2.2.4. n'est pas exactement la correspondance donnée par Hecke ([6] § 53). On peut déduire la correspondance de Hecke de la correspondance du théorème 2.2.4. En effet :

Comparaison des deux correspondances.

1) Correspondance du théorème 2.2.4.

- L'ensemble d'idéaux est l'ensemble I_α des idéaux $\neq (o)$ de F_α. Il est muni de la relation d'équivalence T_1 définie comme suit :

$$E \; T_1 \; E' \iff (\exists \; f' \in Q(\sqrt{\alpha}) \; , \; E' = f' \; E)$$

- L'ensemble de formes est l'ensemble Φ_α^1 des formes quadratiques binaires à coefficients dans $\mathbb{Z}$ de discriminant 4α, il est muni de la relation d'équivalence R_1 définie comme suit :

$Q_1 \; R_1 \; Q_1'$ $\iff$ (Q_1' est équivalente à Q_1 selon R (équivalence ordinaire) par l'intermédiaire d'un automorphisme de déterminant 1, ou $-Q_1'$ est équivalente à Q_1 selon R par l'intermédiaire d'un automorphisme de déterminant -1).

On écrira $Q_1 \; R_1 \; Q_1' \iff (Q_1 \underset{\text{dét } 1}{R} Q_1'$ ou $Q_1 \underset{\text{dét } -1}{R} -Q_1')$

- Soit E un élément de I_α, la classe de formes associée à la classe de E est l'ensemble des formes Q_1 définies comme suit : A chaque base (e_1,e_2) de E on associe la forme Q_1 définie par $Q_1(x,y) = \frac{N_\alpha(xe_1+ye_2)}{\delta}$ où δ est le déterminant de la base (e_1,e_2) relatif à la base $(1,\sqrt{\alpha})$ de F_α.

Correspondance de Hecke.

- L'ensemble d'idéaux est l'ensemble I_α, il est muni de la relation

d'équivalence T_2 définie comme suit :

$E\ T_2\ E' \iff (\exists\ f' \in Q(\sqrt{\alpha}),\ E' = f'\ E$ et $N_\alpha(f') > o)$ (relation restreinte).

Il est immédiat que sur I_α, $E\ T_2\ E'$ implique $E\ T_1\ E'$.

- Lorsque $Q(\sqrt{\alpha})$ est réel, $(\alpha>o)$, l'ensemble de formes est l'ensemble Φ_α^1 précédent. Lorsque $Q(\sqrt{\alpha})$ est imaginaire, $(\alpha<o)$, l'ensemble de formes est la partie de Φ_α^1 constituée par les formes définies positives de Φ_α^1.

Dans les deux cas l'ensemble de formes est muni de la relation d'équivalence R_2 définie comme suit :

$Q_1\ R_2\ Q_1' \iff Q_1\ R_{\text{dét}1}\ Q_1'$ (relation restreinte)

Il est immédiat que sur Φ_α^1, $Q_1\ R_2\ Q_1'$ implique $Q_1\ R_1\ Q_1'$.

- Soit E un élément de I_α, la classe de formes associée à la classe de E est l'ensemble des formes Q_1 définies comme suit : A chaque base (e_1,e_2) de E telle que $\frac{e_1\bar{e}_2 - e_2\bar{e}_1}{\sqrt{4\alpha}}$ soit $> o$ où $\bar{e}_1$ et $\bar{e}_2$ sont les conjugués de e_1 et e_2 (c'est-à-dire telle que le déterminant δ de (e_1,e_2) soit $< o$ car $e_1\bar{e}_2 - e_2\bar{e}_1 = -\delta\sqrt{4\alpha}$) on associe la forme Q_1 définie par $Q_1(x,y) = \frac{N_\alpha(xe_1+ye_2)}{|\delta|}$.

On peut déduire la correspondance de Hecke de la correspondance du théorème 2.2.4. En effet :

Remarques préliminaires :

Remarque 1.

Les relations R_1 et R_2 sont identiques sur Φ_α^1 si et seulement si le corps $Q(\sqrt{\alpha})$ contient une unité (élément inversible de F_α) de norme -1. En effet :

- R_1 et R_2 sont identiques si et seulement si pour tout élément Q_1

de Φ_α^1 , $Q_1 \underset{\text{dét}-1}{R} - Q_1$. En effet :

On suppose que pour tout élément Q_1 de Φ_α^1 , $Q_1 \underset{\text{dét}-1}{R} - Q_1$, alors pour tout couple (Q_1,Q_1') d'éléments de Φ_α^1 tel que $Q_1' \underset{\text{dét}-1}{R} - Q_1$, Q_1' et Q_1 sont équivalentes selon R par le produit de deux automorphismes de déterminant -1 donc on a $Q_1' R Q_1$, donc $Q_1' R_1 Q_1$ implique $Q_1' R_2 Q_1$ comme d'autre part $Q_1' R_2 Q_1$ implique $Q_1' R_1 Q_1$ les relations coïncident.

Inversement on suppose que les deux relations coïncident. Il est immédiat qu'à toute forme Q_1 on peut associer une forme Q_1' telle que $Q_1' \underset{\text{dét}-1}{R} - Q_1$, comme on a aussi $Q_1' \underset{\text{dét}1}{R} Q_1$, $Q_1 \underset{\text{dét}-1}{R} - Q_1$.

- D'autre part on a $Q_1 \underset{\text{dét}-1}{R} - Q_1$ pour tout élément Q_1 de Φ_α^1 si et seulement si le corps $\mathbb{Q}(\sqrt{\alpha})$ contient une unité de norme -1. En effet :

Tout élément Q_1 de Φ_α^1 est défini par $Q_1(x,y) = \dfrac{N_\alpha(xe_1+ye_2)}{\delta}$ où (e_1,e_2) est une base de déterminant δ d'un idéal E de F_α. Lorsque $Q(\sqrt{\alpha})$ contient une unité ε de norme - 1, $(\varepsilon e_1, \varepsilon e_2)$ est une base de E, l'automorphisme σ de E défini par $\sigma(e_1) = \varepsilon e_1$ et $\sigma(e_2) = \varepsilon e_2$ a pour déterminant - 1 et la forme Q_1' équivalente à Q_1 selon R par cet automorphisme est $- Q_1$ (car $\dfrac{N_\alpha(\varepsilon e_1)}{\delta} = - \dfrac{N_\alpha(e_1)}{\delta}$ et $\dfrac{N_\alpha(\varepsilon e_2)}{\delta} = - \dfrac{N_\alpha(e_2)}{\delta}$)

Inversement soit $Q_1 \in \Phi_\alpha^1$ tel que $Q_1 \underset{\text{dét}-1}{R} - Q_1$ et soient E un idéal de F_α et (e_1,e_2) une base de E tels que $Q_1(x,y) = \dfrac{N_\alpha(xe_1+ye_2)}{\delta}$, $-\delta Q_1$ est l'expression de la forme norme sur E relativement à une base (e_1',e_2') de déterminant $\delta' = - \delta$ telle que $N_\alpha(e_1') = - N_\alpha(e_1)$ et $N_\alpha(e_2') = - N_\alpha(e_2)$ (car $\delta Q_1 \underset{\text{dét}-1}{R} - \delta Q_1$) . Soit σ l'automorphisme de E défini par $\sigma(e_1) = e_1'$ et $\sigma(e_2) = e_2'$ alors pour tout couple (x,y) d'éléments de Z, $N_\alpha(xe_1+ye_2) = - N_\alpha(xe_1'+ye_2') = - N_\alpha(\sigma(xe_1+ye_2))$ donc il existe un élément ε de $\mathbb{Q}(\sqrt{\alpha})$ de norme - 1 tel que $E = \varepsilon E$ (c'est une conséquence de la proposition 2.1.2. Puisque $\delta' = -\delta$ l'extension à $\mathbb{Q}(\sqrt{\alpha})$ de l'automorphisme σ est simplement la multiplication par ε). D'autre part, E un module complet au sens de

[5] et ε appartient au stabilisateur de E, $(E = \varepsilon E)$, donc ε appartient à l'anneau des entiers F_α de $\mathbb{Q}(\sqrt{\alpha})$ ([5] p. 98 et 101).

En définitive, lorsque $\mathbb{Q}(\sqrt{\alpha})$ n'a pas d'unité de norme - 1, on n'a jamais $Q_1 \underset{\text{dét}-1}{R} - Q_1$, les relations R_1 et R_2 sont distinctes et chaque classe suivant R_1 est la réunion de deux classes suivant R_2. Lorsque $\mathbb{Q}(\sqrt{\alpha})$ possède une unité de norme - 1, les relations R_1 et R_2 coïncident et pour toute forme Q_1 on a $Q_1 \underset{\text{dét}-1}{R} - Q_1$.

Remarque 2.

Soient E un élément de I_α, (e_1,e_2) une base de E de déterminant $\delta < o$ et Q_1 le représentant associé à (e_1,e_2) de la classe de formes associée à E par le théorème 2.2.4, $(Q_1(x,y) = \frac{N_\alpha(xe_1+ye_2)}{\delta})$, alors $-Q_1$ est une des formes associée par Hecke à l'idéal E.

De plus la forme $-Q_1$ est associée par la correspondance 2.2.4. à l'idéal $\bar{E}$ de base $(\bar{e}_1,\bar{e}_2)$ conjuguée de la base (e_1,e_2) de E. On en déduit que les classes selon R_1 des formes Q_1 et $-Q_1$ sont confondues si et seulement si tout idéal conjugué d'un élément de la classe de E selon T_1 appartient aussi à cette classe. (l'ensemble des formes opposées aux formes d'une classe suivant R_1, (resp. R_2), est toujours une classe suivant R_1 (resp. R_2)).

On peut maintenant envisager trois cas

Cas 1. $\mathbb{Q}(\sqrt{\alpha})$ est réel et possède une unité ε de norme - 1.

Deux idéaux équivalents selon T_1 sont équivalents selon T_2 (en effet $E' = f' E$ avec $N(f') < o$ implique $E' = (f'\varepsilon)E$ avec $N(f'\varepsilon) > o$) T_1 et T_2 sont donc identiques sur I_α.

D'après la remarque 1, R_1 et R_2 coïncident sur Φ_α^1. A toute classe d'idéaux $\tilde{E}$ la bijection du théorème 2.2.4. fait correspondre une classe de formes $\tilde{Q}_1$, la classe $-\tilde{Q}_1$ des formes opposées est l'ensemble des formes associées à E par la correspondance de Hecke, c'est aussi la classe associée aux

idéaux de $\tilde{E}$. L'application $\tilde{E} \to -\tilde{Q}_1$ est une bijection qui est la correspondance de Hecke.

Cas 2. $\mathbb{Q}(\sqrt{\alpha})$ est imaginaire.

Il est connu que dans ce cas les relations T_1 et T_2 coïncident sur I_α. Puisque le corps $\mathbb{Q}(\sqrt{\alpha})$ ne contient pas d'unité de norme - 1, chaque classe de Φ_α^1 selon R_1 se décompose en deux classes suivant R_2, l'une composée des formes définies positives, l'autre des formes définies négatives.

Dans la correspondance de Hecke, l'ensemble de formes est la partie de Φ_α^1 composée des formes définies positives. Soit $\tilde{Q}_1$ la classe de formes suivant R_1 associée à une classe d'idéaux $\tilde{E}$ par le théorème 2.2.4 et $\tilde{Q}_{1(-)}$ l'ensemble des formes négatives de cette classe. L'ensemble $-\tilde{Q}_{1(-)}$ des formes opposées aux formes de $\tilde{Q}_{1(-)}$ est la classe de formes suivant R_2 associée par Hecke à l'idéal E. C'est aussi la classe associée aux idéaux de $\tilde{E}$. L'application $\tilde{E} \to -\tilde{Q}_{1(-)}$ est une bijection qui est la correspondance de Hecke.

Cas 3. $\mathbb{Q}(\sqrt{\alpha})$ est réel et n'a pas d'unité de norme - 1.

Il est connu que dans ce cas chaque classe suivant T_1 d'éléments de I_α est la réunion de deux classes suivant T_2. Puisque $\mathbb{Q}(\sqrt{\alpha})$ n'a pas d'unité de norme - 1, chaque classe d'éléments de Φ_α^1 selon R_1 est la réunion de deux classes selon R_2.

A un élément E de I_α on associe la classe $-\tilde{Q}_1$ selon R_1 comme dans les autres cas. Il est immédiat que les deux classes selon R_2 dont la réunion est $-\tilde{Q}_1$ correspondent l'une aux bases de E de déterminant $> o$, l'autre aux bases de déterminant $< o$ cette dernière est la classe associée à E par la correspondance de Hecke.

Soit $E' \in I_\alpha$ tel que $E' = f'E$. Aux bases (e_1, e_2) de E et $(f'e_1, f'e_2)$ de E' correspond la même forme $-Q_1$ dans $-\tilde{Q}_1$. Lorsque $N_\alpha(f') > o$, les déterminants des deux bases ont même signe donc à E et E' correspond la

même classe de Hecke, lorsque $N_\alpha(f') < o$, les déterminants de ces bases ont des signes opposés donc à E et E' correspondent deux classes de Hecke distinctes. Ce qui prouve de nouveau la bijection de Hecke.

CHAPITRE III

ALGEBRES UNITAIRES DE RANG 2 .

---

§ 1 - *Structures d'algèbre unitaire sur un A-module quadratique projectif de rang 2.*

On utilisera dans ce paragraphe des méthodes de localisation et globalisation.

Notations 3.1.0. (*Cf. B.A.C. Ch. II*)

Pour tout A-module M et tout idéal premier p de A, on note A_p l'anneau local de A en p et M_p le A_p-module $M \otimes_A A_p$.

L'unité de A_p est notée 1_p et l'image d'un élément a de A par l'homomorphisme canonique de A dans A_p est notée $\frac{a}{1_p}$. ($\frac{1}{1_p} = 1_p$)

On désigne par f_p l'homomorphisme canonique de M dans M_p. (f_p est défini pour tout élément X de M par $f_p(X) = X \otimes_A 1_p$).

On désigne par Spec A le spectre de A (ensemble des idéaux premiers).

Rappel : *Théorème* 3.1.1. (*Cf. B.A.C. Ch. II*).

Soient M un A-module et N un sous A-module de M. Pour qu'un élément X de M appartienne à N, il faut et il suffit que pour tout $p \in \text{Spec } A$, l'image canonique de X dans M_p appartienne au sous A_p-module N_p de M_p. En particulier pour que les éléments X et Y de M soient confondus, il faut et il suffit que pour tout $p \in \text{Spec } A$, X et Y aient même image canonique dans M_p.

Remarque.-

Le théorème 3.1.1. est vrai en particulier pour le A_p-module $A \otimes_A A_p$ que l'on identifie à A_p.

1 - Extension du théorème 1.1.1. du chapitre I aux modules projectifs de rang 2.

Proposition 3.1.2.-

Soit E une A-algèbre projective de rang 2, d'unité e. E est associative et commutative. A tout élément X de E, on peut associer sa norme N(X), déterminant de l'endomorphisme $m_X : Y \to XY$ de E, et l'application $N : X \to N(X)$ est une forme quadratique définie sur E, telle que N(e) = 1.

Tout élément X de E vérifie l'équation

$$X^2 + N(X)e - B_N(X,e)X = 0.$$

Preuve.

E est un A-module de type fini tel que pour tout $p \in \operatorname{Spec} A$ E_p soit un A_p-module libre de rang 2. Pour tout $p \in \operatorname{Spec} A$, l'algèbre obtenue par extension des scalaires à A_p est une algèbre quadratique (libre de rang 2), elle est donc associative et commutative. Pour tout $p \in \operatorname{Spec} A$, l'homomorphisme canonique f_p de E dans E_p (not. 3.1.0) est un homomorphisme de A-algèbres. On en déduit grâce au théorème de globalisation, (th. 3.1.1), que E est aussi associative et commutative. En effet, pour montrer que E est associative par exemple, on constate que,

$$\forall p \in \operatorname{Spec} A, \forall X,X' \text{ et } X'' \in E,\ f_p((XX')X'') = (f_p(X)f_p(X'))f_p(X'') =$$

$$= f_p(X)(f_p(X')f_p(X'')) = f_p(X(X'X''))$$

$(XX')X''$ et $X(X'X'')$ ont même image canonique dans E_p pour tout $p \in \operatorname{Spec} A$, ils sont donc égaux d'après le théorème de globalisation.

D'autre part, l'application $m_X : Y \to YY$ est un A-endomorphisme de E, on peut donc lui associer son déterminant N(X). Alors, pour tout $p \in \operatorname{Spec} A$, $\frac{N(X)}{1_p} = N_p(f_p(X))$ où N_p est la norme sur E_p. (Cf. B.A.C. Ch. II § 5, ex. 9)

pour les modules projectifs de rang fini ou $[\,]$ pour les modules projectifs de type fini). On vérifie aisément que N est une forme quadratique définie sur E telle que N(e) = 1. La forme bilinéaire associée B_N est telle que pour tout couple

(X,Y) d'éléments de E et pour tout $p \in \operatorname{Spec} A$, $\dfrac{B_N(X,Y)}{1_p} = B_{N_p}(f_p(X),f_p(y))$.

De plus (prop. 1.1.0) on a pour tout $X \in E$ et tout $p \in \operatorname{Spec} A$,

$$(f_p(X))^2 + N_p(f_p(X))\, f_p(e) - B_{N_p}(f_p(X),f_p(e))\, f_p(X) = 0$$

c'est-à-dire

$$(f_p(X))^2 + \frac{N(X)}{1_p} f_p(e) - \frac{B_N(X,e)}{1_p} f_p(X) = 0$$

et par suite

$$f_p(X^2 + N(X) - B_N(X,e)X) = 0 .$$

Donc, d'après le théorème de globalisation tout élément X de E vérifie l'équation

$$X^2 + N(X)e - B_N(X,e) = 0 .$$

Corollaire.

Toute A-algèbre unitaire E projective de rang 2 est une N-algèbre (déf. 0.1.2) pour la norme N. Toute forme quadratique Q définie sur E pour laquelle E est une Q-algèbre coïncide avec la norme N.

E est une N-algèbre. C'est une conséquence immédiate de la proposition 3.1.2.

Toute forme quadratique Q définie sur une algèbre quadratique E et pour laquelle E est une Q-algèbre coïncide avec la norme N de E (corollaire de la proposition 1.1.0). Cette propriété est encore vraie lorsque E est une algèbre unitaire projective de rang 2. (On le voit en localisant puis en globalisant).

On peut donc poser le problème 1 du chapitre I pour les modules quadratiques projectifs de rang 2.

Problème 1.

Soit (E,Q) un A-module quadratique projectif de rang 2. Peut-on définir sur E une structure de A-algèbre unitaire telle que, N désignant la norme de l'algèbre on ait, pour tout élément X de E, Q(X) = N(X), ou ce qui est équivalent telle que E soit une Q-algèbre pour cette structure ?

Les résultats sont analogues aux résultats du chapitre I.

Théorème 3.1.3.- (Théorème d'existence et d'unicité).

Soit (E,Q) un A-module quadratique projectif de rang 2.
Pour qu'il existe sur E une structure de Q-algèbre (autrement dit pour que le problème 1 admette une solution), il faut et il suffit que la forme Q représente 1.

- Si e est l'unité d'une algèbre solution, Q(e) = 1. Inversement, à tout élément e de E tel que Q(e) = 1, on peut faire correspondre une algèbre solution et une seule d'unité e.

- Les algèbres solutions sont isomorphes.

Remarque 1.

Il existe des modules projectifs de rang 2 munis d'une forme quadratique qui représente 1 qui ne sont pas libres.

Exemple.- A est un anneau de Dedekind qui n'est pas principal, $E = A \oplus I$ où I est un idéal non principal de A. On munit E de la forme quadratique Q définie pour tout élément a+b de E ($a \in A$, $b \in I$) par $Q(a+b) = a^2$.

Le théorème 3.1.3. est donc une généralisation du théorème 1.1.1. du chapitre I.

Preuve du théorème 3.1.3.

On utilise plusieurs lemmes.

Le premier lemme donne une condition nécessaire d'existence et établit l'unicité à isomorphisme près.

Lemme 1.-

Soit (E,Q) un A-module quadratique projectif de rang 2. Pour qu'on puisse munir E d'une structure de Q-algèbre, il faut que la forme Q représente 1.

- Si e est l'unité d'une solution, $Q(e) = 1$. Inversement, pour tout élément e de E tel que $Q(e) = 1$, il existe au plus une algèbre solution d'unité e.

- Les solutions éventuelles sont des A-algèbres isomorphes.

Preuve du lemme 1.

Si e est l'unité d'une solution E_e, $Q(e) = 1$ (déf. 0.1.2) et on vient de voir que Q est la norme de E_e.

- Soit e fixé tel que $Q(e) = 1$ et soit E_e une solution d'unité e. Pour tout $p \in \operatorname{Spec} A$, l'algèbre $(E_p)_e$ obtenue par extension des scalaires à A_p est l'unique A_p-algèbre quadratique de module sous-jacent E_p, d'unité $f_p(e)$ (notations 3.1.0), de norme Q_p où Q_p est l'extension de la forme Q à E_p.

Donc, pour tout $p \in \operatorname{Spec} A$ et tout couple (X_1,X_2) d'éléments de E, $f_p(X_1)f_p(X_2)$, c'est-à-dire $f_p(X_1X_2)$, est indépendant du choix de la solution d'unité e. L'unicité résulte alors du théorème de globalisation 3.1.1.

- On montre maintenant que lorsque E_e (resp. $E_{e'}$) est une Q-algèbre solution d'unité e, (resp. e'), la multiplication par e' pour la structure de E_e est un isomorphisme d'algèbres de E_e sur $E_{e'}$.

Il est immédiat que cette multiplication est un automorphisme du A-module E, l'automorphisme inverse étant la multiplication par e pour la structure de $E_{e'}$. Pour tout couple (X_1,X_2) d'éléments de E, on note X_1X_2 le produit dans E_e et $X_1 \circ X_2$ le produit dans $E_{e'}$. Il s'agit de montrer que $(X_1e') \circ (X_2e') = (X_1X_2)e'$.

Pour tout $p \in \operatorname{Spec} A$, on utilise le même signe de multiplication dans E_e, (resp. $E_{e'}$), et dans l'algèbre $(E_p)_e$, (resp. $(E_p)_{e'}$). Alors, puisque la

multiplication par $f_p(e')$ est un isomorphisme d'algèbres de $(E_p)_e$ sur $(E_p)_{e'}$, (prop. 1.1.2.),

$$f_p((X_1e')o(X_2e')) = f_p(X_1e') \circ f_p(X_2e') = (f_p(X_1)f_p(e')) \circ (f_p(e')) = f_p(X_1X_2)f_p(e')$$

Donc $(X_1e') \circ (X_2e') = (X_1X_2)e'$.

On en déduit que les algèbres E_e et $E_{e'}$ sont isomorphes.

Le lemme suivant donne une première condition nécessaire et suffisante d'existence de solutions.

Lemme 2.-

Soit (E,Q) un A-module quadratique projectif de rang 2. On suppose qu'il existe un élément e de E tel que $Q(e) = 1$. Pour qu'il existe sur E une structure de Q-algèbre d'unité e, il faut et il suffit qu'il existe une application A-bilinéaire ϕ de E^2 dans E telle que, (avec les notations 3.1.0.),

$$\forall\, p \in \operatorname{Spec} A,\ \forall\, X \text{ et } X' \in E,\ f_p(\phi(X,X')) = f_p(X)\, f_p(X')$$

pour la structure de l'algèbre quadratique $(E_p)_e$ d'unité $f_p(e)$, de norme Q_p où Q_p est l'extension de Q à E_p.

Alors E, muni de la multiplication $(X,X') \mapsto XX' = \phi(X,X')$ est une Q-algèbre d'unité e.

Preuve du lemme 2.

- On a déjà vu que cette condition est nécessaire (preuve du lemme 1).

- Elle est suffisante. En effet, il résulte du théorème de globalisation que lorsque cette condition est vérifiée, E est muni d'une structure d'algèbre d'unité e telle que, pour tout $p \in \operatorname{Spec} A$, l'algèbre quadratique $(E_p)_e$ soit l'algèbre obtenue par extension des scalaires à A_p. Donc, si N est la norme sur E, $\forall\, p \in \operatorname{Spec} A$, $\forall\, X \in E$, $\frac{N(X)}{1_p} = N_p(f_p(X))$ où N_p est la norme de E_p. Comme d'autre part, $N_p(f_p(X)) = Q_p(f_p(X)) = \frac{Q(X)}{1_p}$, $N(X)$ et $Q(X)$ ont même image

canonique dans A_p pour tout $p \in \text{Spec } A$. Donc $Q(X) = N(X)$ et E est muni d'une structure de Q-algèbre d'unité e.

Pour prouver le théorème 3.1.3., il suffit de montrer, compte tenu des lemmes 1 et 2, qu'à tout élément e de E tel que $Q(e) = 1$ on peut associer une application A-bilinéaire ϕ vérifiant la condition du lemme 2.

L'existence de cette application est une conséquence des deux lemmes suivants. Le premier est un lemme trivial sur l'extension des scalaires dans les algèbres quadratiques, le second est un exercice de Bourbaki (B.A.C. Ch. II § 5, ex. 9).

Lemme 3.-

Soient (E,Q) un A-module quadratique et S et T deux parties multiplicatives de A tels que S soit contenue dans T et que $S^{-1}E$ soit un $S^{-1}A$-module libre de rang 2.

- Lorsque $0 \in T$, $T^{-1}E$ est nul.

- Lorsque $0 \notin T$, $T^{-1}E$ est un $T^{-1}A$-module libre de rang 2.

Lorsqu'il existe $e \in E$ tel que $Q(e) = 1$, on désigne par $(S^{-1}E)_e$ (resp. $(T^{-1}E)_e$), l'algèbre quadratique d'unité $f_S(e)$ (resp. $f_T(e)$), et de norme Q_S (resp. Q_T), où f_S (resp. f_T), est l'homomorphisme canonique de E dans $S^{-1}E$ (resp. $T^{-1}E$), et Q_S (resp. Q_T), l'extension à $S^{-1}E$ (resp. $T^{-1}E$), de la forme Q. Alors, l'homomorphisme canonique de $S^{-1}E$ dans $T^{-1}E$ est compatible avec les multiplications de $S^{-1}E$ et $T^{-1}E$.

Lemme 4.-

Soient A un anneau commutatif unitaire, $(s_i)_{i \in I}$ une famille finie d'éléments de A engendrant l'idéal A, E un A-module. S_i (resp. S_{ij}), désignant la partie multiplicative de A engendrée par s_i (resp. s_i et s_j), on pose $S_i^{-1}A = A_{s_i}$, $S_i^{-1}E = E_{s_i}$, $S_{ij}^{-1}A = A_{s_is_j}$, $S_{ij}^{-1}E = E_{s_is_j}$. On suppose donné dans chacun des A_{s_i}-modules E_{s_i} un élément Z_i tel que, pour tout couple (i,j)

d'éléments de I, les images canoniques de Z_i et Z_j dans $E_{s_i s_j}$ soient égales. Alors, il existe un élément Z de E et un seul tel que, pour tout $i \in I$, l'image canonique de Z dans E_{s_i} soit égale à Z_i.

Soit (E,Q) un A-module quadratique projectif de rang 2 et soit $e \in E$ tel que $Q(e) = 1$. On peut maintenant démontrer l'existence d'une application bilinéaire ϕ vérifiant les hypothèses du lemme 2.

Puisque E est projectif de rang 2, il existe une famille finie $(s_i)_{i \in I}$ d'éléments de A engendrant l'idéal A telle que, pour tout $i \in I$, E_{s_i} soit un A_{s_i}-module libre de rang 2 (B.A.C. Ch. II).

Pour tout $i \in I$ et tout $X \in E$, on désigne par X_i l'image canonique de X dans E_{s_i} et pour tout couple (i,j) d'éléments de I, on désigne par X_{ij} l'image canonique de X dans $E_{s_i s_j}$.

Puisqu'il existe un élément e de E tel que $Q(e) = 1$, pour tout $i \in I$, E_{s_i} est muni de la structure d'algèbre quadratique $(E_{s_i})_e$ d'unité e_i de norme Q_{s_i}, où Q_{s_i} est l'extension de Q à E_{s_i}. Soient X et X' deux éléments de E. Pour tout $i \in I$, on désigne par Z_i, le produit de X_i et X'_i dans $(E_{s_i})_e$. Alors, la famille $(Z_i)_{i \in I}$ vérifie l'hypothèse du lemme 4.

En effet, soient i et j deux éléments de I.

- Lorsque $s_i s_j$ est un élément nilpotent de A, les images canoniques de Z_i et Z_j dans $E_{s_i s_j}$ sont nulles.

- Lorsque $s_i s_j$ n'est pas nilpotent, $E_{s_i s_j}$ est muni de la structure d'algèbre quadratique $(E_{s_i s_j})_e$ d'unité e_{ij} et de norme $Q_{s_i s_j}$ où $Q_{s_i s_j}$ est l'extension de Q à $E_{s_i s_j}$. D'après le lemme 3, Z_i et Z_j ont pour image canonique dans $(E_{s_i s_j})_e$ le produit dans $(E_{s_i s_j})_e$ des éléments X_{ij} et X'_{ij}.

Soit Z l'élément de E associé à la famille $(Z_i)_{i \in I}$ par le lemme 4. On pose $\phi(X,X') = Z$.

L'application $\phi : E^2 \to E$ ainsi définie vérifie les conditions du lemme 2. En effet :

Soit $p \in \operatorname{Spec} A$, puisque la famille $(s_i)_{i \in I}$ engendre l'idéal A,

il existe au moins un élément i de I tel que s_i appartienne à $A-p$. On sait que dans $(E_{s_i})_e$ $Z_i = X_i X_i'$, on en déduit, en utilisant le lemme 3 avec $T = A-p$, que $f_p(Z) = f_p(X) f_p(X')$. Donc

$$\forall\, p \in \operatorname{Spec} A, \quad X \text{ et } X' \in E, \quad f_p(\phi(X,X')) = f_p(X)\, f_p(X')$$

Il est immédiat que ϕ est A-bilinéaire.

Remarque 2.

La preuve du théorème 3.1.3. peut être simplifiée dans le cas où, S désignant l'ensemble des éléments réguliers de A, $S^{-1}E$ est libre de rang 2. Elle est immédiate lorsque A est intègre car E peut être identifié à l'intersection des E_p.

Remarque 3.

(E,Q) désignant un A-module quadratique projectif de rang 2, on suppose que la propriété (1.2.10)' ci-dessous est vérifiée (cf. Chap. I).

(1.2.10)' | Il existe une forme bilinéaire B_1 définie sur E^2 telle que, pour tout élément X de E, $Q(X) = B_1(X,X)$.

Alors, lorsqu'il existe $e \in E$ tel que $B_1(e,e) = 1$, la multiplication de la Q-algèbre E_e associée à e selon le théorème 3.1.3. est définie pour tout couple (X,X') d'éléments de E par

$$XX' = - B_1(X,X')e + B_1(X,e)X' + B_1(X',e)X$$

De plus, E est la somme directe du module libre Ae et du module projectif de rang 1 $(Ae)^{\perp_1}$, orthogonal de Ae pour la forme B_1.

En effet, la forme bilinéaire associée à Q est $2B_1$, il est immédiat que pour la multiplication définie ci-dessus, E est muni d'une structure de Q-algèbre d'unité e. Cette algèbre est la solution unique du problème 1 associée à e.

Pour montrer que E est la somme directe de Ae et de son orthogonal $(Ae)^{\perp_1}$ pour B_1 où Ae est libre et $(Ae)^{\perp_1}$ projectif de rang 1, on utilise

le résultat analogue pour les modules libres (prop. (1.2.10')) et une méthode de localisation et globalisation. Lorsque la propriété (1.2.10') est vérifiée et lorsque de plus A est intègre le A-module E est isomorphe à $A \oplus I$ avec I idéal fractionnaire inversible de A.

On revient à l'étude générale des solutions du problème 1.

2 - Etude des isomorphimes.

Les propositions 1.1.2. et 1.1.3. du chapitre I et leurs conséquences sont vraies aussi lorsque E est un A-module projectif de rang 2.

Exemple de preuve.

Proposition 3.1.4.- (Prop. 1.1.2. du chapitre I).

Soit (E,Q) un A-module quadratique projectif de rang 2. On suppose qu'il existe deux éléments e et e' de E tels que $Q(e) = Q(e') = 1$ et on désigne par E_e et $E_{e'}$ les Q-algèbres solutions du problème 1 associées à e et e' respectivement selon le théorème 3.1.3.

Il y a identité entre l'ensemble $\sum_{ee'}$ des isomorphismes d'algèbres de E_e sur $E_{e'}$ et l'ensemble des transformations orthogonales σ de (E,Q) telles que $\sigma(e) = e'$.

Preuve.

Soit E_e (resp. $E_{e'}$) la Q-algèbre solution du problème 1 d'unité e (resp. e'). Pour tout $p \in \operatorname{Spec} A$, on désigne par $(E_p)_e$ (resp. $(E_p)_{e'}$), l'algèbre obtenue par extension des scalaires à A_p, c'est-à-dire l'algèbre quadratique d'unité $f_p(e)$, (resp. $f_p(e')$), et de norme Q_p où Q_p est l'extension de Q à E_p (notations 3.1.0.).

Soit σ un automorphisme du A-module E. Pour tout $p \in \operatorname{Spec} A$, on désigne par σ_p l'extension de σ à E_p ($\sigma_p = \sigma \otimes 1_{A_p}$). Les propriétés suivantes sont équivalentes.

(1) σ est une transformation orthogonale de (E,Q) telle que $\sigma(e) = e'$

(2) Pour tout $p \in \mathrm{Spec}\, A$, σ_p est une transformation orthogonale de (E_p,Q_p) telle que $\sigma_p(f_p(e)) = f_p(e')$.

(3) Pour tout $p \in \mathrm{Spec}\, A$, σ_p est un isomorphisme de l'algèbre $(E_p)_e$ sur l'algèbre $(E_p)_{e'}$.

(4) σ est un isomorphisme de l'algèbre E_e sur l'algèbre $E_{e'}$.

En effet :

Puisque E_p est libre de rang 2 sur A_p, l'équivalence de (2) et (3) résulte de la proposition 1.1.2. du chapitre I.

Puisque $\sigma_p(f_p(X)) = f_p(\sigma(X))$ et $\frac{Q(X)}{1}_p = Q_p(f_p(X))$, l'équivalence de (1) et (3) et de (3) et (4) s'obtient par localisation et globalisation.

§ 2 - *Etude d'une algèbre unitaire projective de rang 2.*

Dans tout ce paragraphe, E désigne une algèbre unitaire projective de rang 2, d'unité e, de norme N. On désigne par B la forme bilinéaire associée à N.

On reprend l'étude des propriétés énoncées dans le paragraphe § 2 du chapitre I.

1 - Propriétés préliminaires.

Tout élément X de E vérifie l'équation quadratique

$$X^2 + N(X)e - B(X,e)X = 0 \qquad \text{(prop. 3.1.2.)}.$$

Il est immédiat que l'application $\sigma : X \to B(X,e)e - X$ est un automorphisme du A-module E égal à son inverse. De plus la proposition 1.2.1. du chapitre I et ses corollaires sont vrais aussi lorsque E est projectif de rang 2.

Pour la preuve de la proposition 1.2.1. on utilise le procédé de localisation et globalisation précédent. Les preuves des corollaires s'adaptent facilement au cas projectif.

2 - Propriétés relatives à l'ensemble des éléments isotropes et au noyau du module quadratique (E,N).

On définit les ensembles H, K, K_1 comme dans l'introduction et dans le paragraphe 2 du chapitre I (déf. 0.1.1.).

Pour tout $p \in \operatorname{Spec} A$, désigne par N_p la norme de l'algèbre E_p obtenue par extension des scalaires à A_p, par B_p la forme bilinéaire associée.

Avec les notations (3.1.0.) on a,

$$\forall\, p \in \operatorname{Spec} A \quad , \quad \frac{B(X,X')}{1_p} = B_p(f_p(X), f_p(X')) \quad , \quad \frac{N(X)}{1_p} = N_p(f_p(X))$$

donc

$$B(X,X') = 0 \iff \forall\, p \in \operatorname{Spec} A \quad , \quad B_p(f_p(X) \quad , \quad f_p(X')) = 0$$

$$N(X) = 0 \iff \forall\, p \in \operatorname{Spec} A \quad , \quad N_p(f_p(X)) = 0.$$

Il est immédiat que

$$K = \{X \mid X \in E \text{ et } \forall\, p \in \operatorname{Spec} A \quad , \quad \forall\, Y_p \in E_p \quad , \quad B_p(f_p(X), Y_p) = 0\}$$

$$H = \{X \mid X \in E \text{ et } \forall\, p \in \operatorname{Spec} A \quad , \quad N_p(f_p(X)) = 0\}$$

d'où, en désignant par H_p, K_p, $(K_1)_p$ les ensembles analogues relatifs au module quadratique (E_p, N_p)

$$H = \{X \mid X \in E \text{ et } \forall\, p \in \operatorname{Spec} A \quad , \quad f_p(X) \in H_p\}$$

$$K = \{X \mid X \in E \text{ et } \forall\, p \in \operatorname{Spec} A \quad , \quad f_p(X) \in K_p\}$$

$$K_1 = \{X \mid X \in E \text{ et } \forall\, p \in \operatorname{Spec} A \quad , \quad f_p(X) \in (K_1)_p\}$$

En particulier, lorsque A est intègre et lorsqu'on identifie E et les sous-modules E_p à des sous-modules de $E_{(0)}$ (noté E_0 dans le chapitre I),

$$K = \bigcap_{p \in \operatorname{Spec} A} K_p \quad , \quad H = \bigcap_{p \in \operatorname{Spec} A} H_p \quad , \quad K_1 = \bigcap_{p \in \operatorname{Spec} A} (K_1)_p$$

Compte-tenu de ces remarques, il est facile de vérifier que les propositions 1.2.2., 1.2.3., 1.2.4. (avec son corollaire), 1.2.5. du § 2 chapitre I sont vraies aussi lorsque E est projectif de rang 2. Les preuves qui n'utilisent pas une base peuvent être reproduites sans changement. Pour le reste, on utilise un procédé de localisation et globalisation.

La proposition 1.2.6. n'a pas à être généralisée car lorsque A est principal, E est libre.

L'étude faite dans le cas où A est intègre p. 16-17 peut être reprise sans changement.

3 - Etude du groupe d'automorphismes de l'algèbre E.

Soit T le groupe d'automorphismes de l'algèbre E.

D'après la proposition 3.1.4., T est le groupe des transformations orthogonales de (E,N) qui laissent e invariant. Il contient toujours l'automorphisme $X \to B(X,e)e - X$. Dans certains cas, cet automorphisme est confondu avec l'automorphisme identique.

On voit facilement que la proposition 1.2.8. du chapitre I est vraie dans le cas projectif et que la proposition 1.2.9. peut être modifiée comme suit :

Proposition.-

On suppose A intègre.

- Lorsque $K = (0)$, (N non dégénérée), le groupe d'automorphismes T de E a exactement deux éléments, l'identité et l'automorphisme $X \mapsto B(X,e)e - X$.

- Lorsque $K \neq (0)$, l'orbite O_X de chaque élément X de E est contenue dans $X + K_1$.

Dans les deux cas, le groupe T est commutatif.

4 - Problèmes d'orthogonalité.

On a déjà vu que la proposition 1.2.10' est vraie aussi lorsque E est projectif de rang 2 (remarque 3 du théorème 3.1.3.)

Il est facile de vérifier que les propositions (1.2.10.), (1.2.11.), (1.2.11'.) restent vraies lorsqu'on suppose seulement E projectif de rang 2.

Remarque.

Lorsque A est intègre et lorsque $E = A \oplus I$ où I est un idéal inversible de A égal à $(A)^{\perp}$, (resp. $(A)^{\perp_1}$), I n'est pas en général un idéal de E. Pour qu'il en soit ainsi, il faut que I soit contenu dans le noyau K_1 du module quadratique (E,B) (prop. (1.2.11) ou (1.2.11')). Par exemple, lorsque N est définie pour tout élément $a+b$ de E, $(a \in A, b \in I)$, par $N(a+b) = a^2+b^2$, I n'est pas contenu dans le noyau K_1 de (E,N) et n'est pas un idéal de l'algèbre E d'unité $e = 1$, (unité de A), de norme N.

§ 3 - *Algèbres unitaires de rang 2 sur un anneau intègre.*

Notations et conventions 3.3.1.-

Dans ce paragraphe on suppose que l'anneau A est intègre et on désigne par A_0 le corps des fractions de A.

Pour tout A-module E de rang 2, on désigne par E_0 le A_0-module $E \otimes_A A_0$, (E_0 est libre de rang 2), et par f_0 l'homomorphisme canonique de E dans E_0.

On identifie A à son image dans A_0 par l'injection canonique et dans la partie 1 de ce paragraphe (lorsque E est sans torsion), on identifie E à $f_0(E)$.

1 - Structures d'algèbre unitaire sur un A-module quadratique sans torsion de rang 2.

a) Etude d'une algèbre unitaire sans torsion de rang 2 sur A.

Soit E un A-module sans torsion de rang 2 sur A. Lorsque E est muni d'une structure d'algèbre d'unité e, E_0 est muni de la structure de A_0-algèbre quadratique obtenue par extension des scalaires à A_0. La structure d'algèbre de E est induite par la structure d'algèbre de E_0. E est donc associa-

tive et commutative. La norme N_0 de E_0 induit une application de E dans A_0. Soit B_{N_0} la forme bilinéaire associée à N_0, alors, pour tout élément X de E

$$X^2 = - N_0(X)e + B_{N_0}(X,e)X$$

Lorsque la restriction N de N_0 à E est à valeurs dans A, cette restriction est une forme quadratique définie sur le A-module E et il est immédiat que E est une N-algèbre (déf. 0.1.2.). Toute forme quadratique Q pour laquelle E est une Q-algèbre est la restriction de N_0 à E, (en effet, l'extension Q_0 de Q à E_0 coïncide avec N_0).

Mais N n'est pas nécessairement à valeurs dans A.

Exemple. Soit E_0 l'algèbre quadratique sur Q, d'unité e, de base (e,i) telle que $i^2 = \frac{1}{4}e$. On prend pour E la sous Z-algèbre monogène de E_0 engendrée par i. Alors E est sans torsion de rang 2 sur Z et $N_0(i) = -\frac{1}{4}$.

Proposition 3.3.2.-

Soit E une algèbre sans torsion de rang 2 sur A, d'unité e. Pour qu'il existe une forme quadratique Q définie sur E telle que E soit une Q-algèbre, il faut et il suffit que tout élément X de E vérifie une équation quadratique de la forme

$$X^2 = \alpha(X)e + \beta(X)X \quad , \quad (\alpha(X) \quad , \quad \beta(X) \in A) .$$

Lorsque cette condition est vérifiée, Q est la restriction à E de la norme N_0 de l'algèbre quadratique E_0 (not. 3.3.1.).

Preuve.

Il résulte de ce qui précède qu'une condition nécessaire et suffisante pour qu'il existe une forme quadratique Q définie sur E telle que E soit une Q-algèbre est que la restriction N de la norme N_0 de E_0 à E soit à valeurs dans A. Dans ce cas $Q = N$.

Lorsque N est à valeurs dans A, tout élément X de E vérifie l'équation quadratique $X^2 = - N(X)e + B_N(X,e)X$, $(N(X), B_N(X,e) \in A)$.

Pour terminer la preuve de la proposition, il reste à montrer que lorsque tout élément X de E vérifie une équation quadratique de la forme $X^2 = \alpha(X)e + \beta(X)X$, $(\alpha(X),\beta(X), \in A)$, la restriction N de N_0 est à valeurs dans A.

On suppose que tout élément X de E vérifie l'équation quadratique $X^2 = \alpha(X)e + \beta(X)X$, $(\alpha(X), \beta(X) \in A)$.

Tout élément X de E est alors solution dans E_0 des deux équations quadratiques :

$$X^2 = \alpha(X)e + \beta(X)X$$
$$X^2 = - N_0(X)e + B_{N_0}(X,e)X$$

Lorsque e et X forment une base de E_0.

$\alpha(X) = - N_0(X)$, $\beta(X) = B_{N_0}(X,e)$ en particulier $N_0(X) \in A$.

Remarque : $\forall k \in A_0 - \{0\}$, e et kX forment une base de E_0, et lorsque kX est un élément de E, $\beta(kX) = B_{N_0}(kX,e) = kB_{N_0}(X,e) = k\beta(X)$.

Lorsque e et X ne forment pas une base de E_0.

X est de la forme $\frac{a}{b} e$ $(a,b \in A)$ et $N_0(X) = \frac{a^2}{b^2}$. Lorsque $\frac{a}{b} = 0$, $N_0(X) = 0$.

On suppose maintenant $\frac{a}{b} \neq 0$. On montre que $\frac{a^2}{b^2}$ appartient à A. Soit $y \in E$ tel que e et Y forment une base de E_0.

$$(Y + \frac{a}{b} e)^2 = \alpha(Y)e + \beta(Y)Y + 2 \frac{a}{b} Y + \frac{a^2}{b^2} e$$

et $(Y + \frac{a}{b} e)^2 = \alpha(Y + \frac{a}{b} e)e + \beta(Y + \frac{a}{b} e)(Y + \frac{a}{b} e)$

d'où $$\alpha(Y) + \frac{a^2}{b^2} = \alpha(Y + \frac{a}{b} e) + \frac{a}{b} \beta(Y + \frac{a}{b} e)$$

$$\beta(Y) + 2 \frac{a}{b} = \beta(Y + \frac{a}{b} e)$$

On en déduit

$$\alpha(Y) - \alpha(Y + \frac{a}{b} e) - \frac{a}{b} \beta(Y) = + \frac{a^2}{b^2}$$

$\alpha(Y)$ et $\alpha(Y + \frac{a}{b} e)$ appartiennent à A. D'autre part, puisque $\frac{a}{b} e$ et Y appartiennent à E, leur produit $\frac{a}{b} Y$ appartient à E. e et $\frac{a}{b} Y$ forment une base de E_0 donc d'après la remarque précédente $\beta(\frac{a}{b} Y) = \frac{a}{b} \beta(Y)$ et $\frac{a}{b} \beta(Y)$ est un élément de A donc $\frac{a^2}{b^2}$ appartient à A, c'est-à-dire $N_0(X)$ appartient à A.

b) Etude du problème 1 pour les modules quadratiques sans torsion de rang 2 sur A.

On peut poser le problème 1 sous la forme ci-dessous.

Problème 1.

Soit (E,Q) un A-module quadratique sans torsion de rang 2 sur l'anneau intègre A. Peut-on définir sur E une structure de A-algèbre unitaire telle que, N désignant la restriction à E de la norme N_0 de l'algèbre E_0 obtenue par extension des scalaires à A_0 (not. 3.3.1), on ait pour tout élément X de E, $Q(X) = N(X)$, ou, ce qui est équivalent, telle que E soit une Q-algèbre pour cette structure.

Remarques.

- Lorsque E est projectif, N est la norme.

- Il existe des modules sans torsion de rang 2 non projectifs et munis d'une forme quadratique qui représente 1.

Exemple. A est un anneau qui n'est pas de Dedekind, $E = A \oplus I$ où I

est un idéal fractionnaire non inversible et non nul de A. Pour tout élément a+Y de E, (a ε A, y ε I), on pose $Q(a+Y) = a^2$.

Le problème 1 posé ici est donc une généralisation du problème posé pour les modules projectifs de rang 2 sur un anneau intègre.

Pour que le problème 1 admette une solution, il faut que la forme Q représente 1, mais il existe des anneaux A et des modules quadratiques (E,Q) pour lesquels cette condition n'est pas suffisante.

Exemple.

Soit A l'ordre du corps quadratique $Q(\sqrt{3})$ de conducteur 2, ($A = \{a + 2b\sqrt{3} \mid a$ et $b \in Z\}$), et soit $y_0 = 2\sqrt{3}$.

$\frac{y_0}{2}$ est un élément du corps des fractions A_0 de A qui n'appartient pas à A, mais $\frac{y_0^2}{4}$ appartient à A.

Soient $E_0 = A_0 e \oplus A_0 i$, Q_0 la forme quadratique définie sur E_0 par $Q_0(e) = 1$, $B_0(e,i) = 0$, $Q_0(i) = 3$, et E le sous A-module de E_0 engendré par e, i, $\frac{y_0}{2} i$.

- Q_0 induit une forme quadratique Q sur le A-module E.

En effet : soit $X = xe + yi + z\frac{y_0}{2} i$, (x, y, z ε A),

$Q_0(X) = x^2 + 3(y^2 + 3z^2 + 2yz\sqrt{3})$. Donc $Q_0(X)$ appartient à A.

- L'équation Q(X) = 1 admet pour seules solutions X = e et X = -e.

En effet, si $x = a + 2b\sqrt{3}$, $y = a' + 2b'\sqrt{3}$, $z = a'' + 2b''\sqrt{3}$,

$Q(X) = a^2 + 12b^2 + 3\left[(a' + 6b'')^2 + 3(2b' + a'')^2\right] + 3\left[2ab + 2(a' + 6b'')(2b' + a'')\right]\sqrt{3}$

$Q(X) = 1$ exige $a^2 = 1$, $b = a' + 6b'' = 2b' + a'' = 0$.

Donc Q(X) = 1 exige X = e ou X = -e.

- La multiplication de l'algèbre quadratique $(E_0)_e$, (resp. $(E_0)_{-e}$), d'unité e, (resp. -e), de norme Q_0 n'induit pas une loi interne sur E. En effet : Pour X = i et $X' = \frac{y_0}{2} i$, $XX' = -3\sqrt{3}e$, (resp. $3\sqrt{3}e$).

Pour obtenir un théorème d'existence et d'unicité analogue aux théorèmes 1.1.1. et 3.1.3. on va imposer une condition supplémentaire aux modules quadratiques considérés.

Théorème 3.3.3.- (Théorème d'existence et d'unicité).

Soit (E,Q) un module quadratique sans torsion, de rang 2 sur l'anneau intègre A et vérifiant la propriété suivante :

(1.2.10') | Il existe une forme bilinéaire B_1 définie sur E^2 telle que pour tout élément X de E, $Q(X) = B_1(X,X)$.

Pour qu'il existe sur E une structure de Q-algèbre, autrement dit pour que le problème 1 admette une solution, il faut et il suffit que la forme Q représente 1.

- Si e est l'unité d'une solution, $Q(e) = 1$. Inversement, à tout élément e de E tel que $Q(e) = 1$, on peut faire correspondre une algèbre solution et une seule.

- Les algèbres solutions sont isomorphes.

(La propriété (1.2.10') a déjà été rencontrée dans l'étude des modules quadratiques projectifs). La forme bilinéaire associée à Q est $2B_1$).

Preuve.

On a déjà vu que :

- Pour toute solution d'unité e, $Q(e) = 1$.

- A tout élément e de E tel que $Q(e) = 1$ correspond au plus une solution E_0 d'unité e, la structure de E_e étant induite par la structure de l'unique algèbre quadratique $(E_0)_e$ de module sous-jacent E_0, d'unité e, de norme Q_0 extension de Q à E_0.

- D'autre part, puisque la propriété (1.2.10') est vérifiée, il est immédiat que, pour la multiplication définie pour tout couple (X,X') d'éléments de E par

$$XX' = - B_1(X,X')e + B_1(X,e)X' + B_1(X',e)X,$$

E est munie d'une structure de Q-algèbre d'unité e.

- Soient e et e' deux éléments de E tels que $Q(e) = Q(e') = 1$, E_e (resp. $E_{e'}$), la Q-algèbre solution d'unité e (resp. e'), $(E_0)_e$ (resp. $(E_0)_{e'}$) l'algèbre obtenue par extension des scalaires à A_0. La multiplication par e' pour la structure de $(E_0)_e$ est un isomorphisme de $(E_0)_e$ sur $(E_0)_{e'}$, il est facile de voir que sa restriction à E_e est un isomorphisme de A-algèbres de E_e sur $E_{e'}$, l'isomorphisme inverse est la multiplication par e pour la structure de l'algèbre $E_{e'}$.

Tout A-automorphisme de E se prolonge à un A_0-automorphisme de E_0. Il est facile de voir qu'il y a encore identité entre l'ensemble des isomorphismes d'algèbres de E_e sur $E_{e'}$ et l'ensemble des transformations orthogonales de (E,Q) telles que $\sigma(e) = e'$.

Soit E_e une N-algèbre sans torsion de rang 2 sur A, d'unité e. Les propositions 1.2.1., 1.2.3., 1.2.5., l'étude page 17 du chapitre I sont vraies aussi pour E_e. La proposition 1.2.4. est ici une conséquence de la proposition 1.2.5 et la proposition 1.2.9. est vraie sous la forme modifiée du chapitre III § 2. (On utilise les propriétés analogues de l'algèbre $(E_0)_e$)

On voit facilement que les propositions (1.2.10)', (1.2.11) et (1.2.11)' sont vraies aussi pour une N-algèbre sans torsion de rang 2 sur A.

En particulier lorsque le module quadratique (E,Q) est de type fini, vérifie les hypothèses du théorème (3.3.3.) et possède un élément e tel que $Q(e) = 1$, E est A-isomorphe à $Ae \oplus I$ où I est un idéal fractionnaire de A.

2 - Structures d'algèbre unitaire sur un module quadratique de rang 2 sur l'anneau intègre A.

Notations et conventions (3.3.1)'.

On garde les notations et conventions du début de ce paragraphe (déf. 3.3.1.). A_0 désignant le corps des fractions de A, on identifie donc A à son

image dans A_0 par l'injection canonique. Soit E un A-module de rang 2 sur A. Sauf indication contraire, T désigne le sous-module de torsion de E. T est le noyau de l'homomorphisme canonique f_0 de E dans E_0.

Remarque. Il est immédiat que pour toute forme quadratique Q définie sur E, T est contenu dans le noyau du module quadratique (E,Q).

a) Etude d'une algèbre unitaire de rang 2 sur A.

Soit E une algèbre de rang 2 sur A, d'unité e.

L'algèbre E_0 obtenue par extension des scalaires à A_0 est une algèbre quadratique sur A_0, d'unité $f_0(e)$.

Il est immédiat que le sous-module de torsion T de E est un idéal bilatère et que l'algèbre quotient E/T est une A-algèbre isomorphe à la sous A-algèbre $f_0(E)$ de E_0.

La norme N_0 de l'algèbre E_0 induit une application de $f_0(E)$ dans A_0. Lorsque la restriction $\bar{N}$ de N_0 à $f_0(E)$ est à valeurs dans A, cette restriction est une forme quadratique définie sur le A-module $f_0(E)$. On peut alors lui associer la forme quadratique N sur E définie pour tout élément X de E par $N(X) = \bar{N}(f_0(X)) = N_0(f_0(X))$. N est l'unique forme quadratique définie sur E dont l'extension à E_0 est N_0. $N(e) = 1$, mais E n'est pas nécessairement une N-algèbre (déf. 0.1.2.). On donnera des exemples dans la suite. Toutefois :

Proposition 3.3.4.- (Généralisation de la proposition 3.3.2.)

Soit E une algèbre de rang 2 sur l'anneau intègre A, d'unité e. Pour qu'il existe une forme quadratique Q définie sur E telle que E soit une Q-algèbre, il faut et il suffit que tout élément X de E vérifie une équation quadratique de la forme

$$X^2 = \alpha(X)e + \beta(X)X \quad , \quad (\alpha(X),\beta(X) \in A).$$

Lorsque cette condition est vérifiée, Q est l'unique forme quadratique définie sur E dont l'extension à E_0 est la norme N_0 de l'algèbre quadratique E_0.

Preuve.

- Lorsque E est une Q-algèbre, l'algèbre E_0 est une Q_0-algèbre. Donc $Q_0 = N_0$ (corollaire de la proposition 1.1.0.). Donc Q est l'unique forme quadratique définie sur E dont l'extension à E_0 est la norme N_0 de E_0. Avec les notations précédentes, $Q = N$.

- Lorsque E est une Q-algèbre, on a pour tout élément X de E

$$X^2 = - Q(X)e + B(X,e)X \qquad (-Q(X) \ , \ B(X,e) \in A).$$

Il reste à montrer que lorsque tout élément X de E vérifie une équation de la forme

$$X^2 = \alpha(X)e + \beta(X)X \qquad (\alpha(X) \ , \ \beta(X) \in A)$$

E est une N-algèbre.

On suppose que pour tout élément X de E

$$X^2 = \alpha(X)e + \beta(X)X \qquad (\alpha(X) \ , \ \beta(X) \in A)$$

alors, pour tout élément $f_0(X)$ de $f_0(E)$

$$(f_0(X))^2 = \alpha(X)f_0(e) + \beta(X)f_0(X)$$

L'algèbre $f_0(E)$ est sans torsion de rang 2 sur A. La proposition 3.3.2. montre que la restriction à $f_0(E)$ de la norme N_0 de E_0 est à valeurs dans A. On pose, pour tout élément X de E, $N(X) = N_0(f_0(X))$. On va montrer que, pour tout élément X de E,

$$X^2 = - N(X)e + B_N(X,e)X.$$

On sait que

$$\forall \ X \in E, \quad f_0(X^2) = \alpha(X)f_0(e) + \beta(X) \ f_0(X)$$

$$f_0(X^2) = - N(X) \ f_0(e) + B_N(X,e)f_0(X)$$

- Lorsque $f_0(e)$ et $f_0(X)$ forment une base de E_0,

$N(X) = -\alpha(X)$ et $B_N(X,e) = \beta(X)$ donc $X^2 = -N(X)e + B_N(X,e)X$.

- Lorsque $f_0(e)$ et $f_0(X)$ ne forment pas une base de E_0 et lorsque $f_0(X) \neq 0$,

Il existe deux éléments a et b de $A - \{0\}$ tels que $bX = ae$ (en effet, il existe a' et b' ε $A - \{0\}$ tels que $b'f_0(X) = a'f_0(e)$ et $c \varepsilon A - \{0\}$ tel que $c(b'X-a'e) = 0$. On pose $cb' = b$, $ca' = a$).

Soit $Y \varepsilon E$ tel que $f_0(e)$ et $f_0(Y)$ forment une base de E_0, $f_0(e)$ et $f_0(X + bY)$ forment aussi une base de E_0.

On a d'une part, compte-tenu de l'équation $bX = ae$,

$$(X + bY)^2 = X^2 + b^2Y^2 + (bY)X + X(bY) = X^2 + b^2Y^2 + 2aY$$

et d'autre part

$$(X + bY)^2 = -N(X + bY)e + B_N(X + bY,e)(X + bY)$$

$$= -\left[N(X)+N(bY)+B_N(X,bY)\right]e+B_N(X,e)X+B_N(X,e)bY+B_N(bY,e)X+B_N(bY,e)bY$$

ou, compte-tenu de $ae - bX = 0$ et $Y^2 = -N(Y)e + B_N(Y,e)Y$

$$(X + bY)^2 = -N(X)e + B_N(X,e)X + Y^2 + 2aY$$

comme $(X + bY)^2 = X^2 + Y^2 + 2aY$, on a de nouveau

$$X^2 = -N(X)e + B_N(X,e)X$$

- En particulier, pour tout élément Z du sous-module de torsion T

$$(e + Z)^2 = -N(e + Z)e + B_N(e + Z,e)(e + Z) = e + 2Z$$

ce qui implique $Z^2 = 0$ c'est-à-dire $Z^2 = -N(Z)e + B(Z,e)Z$.

Donc E est une N-algèbre.

b) Etude du problème 1 pour les modules quadratiques de rang 2 sur l'anneau intègre A.

Problème 1.

Soit (E,Q) un A-module quadratique de rang 2 sur l'anneau intègre A.

Peut-on définir sur E une structure d'algèbre unitaire telle que E soit une Q-algèbre pour cette structure ?

D'après la proposition 3.3.4., toute solution du problème 1 est une solution du problème suivant :

Problème 3.3.5.-

Soit (E,Q) un A-module quadratique de rang 2 sur l'anneau intègre A. Peut-on définir sur E une structure d'algèbre unitaire telle que N_0 désignant la norme de l'algèbre quadratique obtenue par extension des scalairas à A_0, on ait pour tout élément X de E, $Q(X) = N_0(f_0(X))$ (avec les notations 3.3.1.).

Comme dans la partie 1 de ce paragraphe, on ne considère que les modules quadratiques (E,Q) vérifiant la propriété (1.2.10)'.

Proposition 3.3.6.-

Soit (E,Q) un module quadratique de rang 2 sur l'anneau intègre A vérifiant la propriété suivante

(1.2.10)' | Il existe une forme bilinéaire B_1 définie sur E^2 telle que pour tout élément X de E, $Q(X) = B_1(X,X)$.

Pour toute solution d'unité e du problème 3.3.5., $Q(e) = 1$. Inversement, à tout élément e de E tel que $Q(e) = 1$, on peut faire correspondre au moins une algèbre solution du problème 3.3.5. d'unité e.

Preuve.

On utilise les notations et conventions (3.3.1.)'. On a déjà vu que pour toute solution d'unité e, $Q(e) = 1$. Soit e un élément de E tel que $Q(e) = 1$ et soit Q_0 l'extension de la forme Q à E_0. Alors $Q_0(f_0(e)) = 1$. D'après le théorème 3.3.3. il existe sur $f_0(E)$ une structure unique de A-algèbre d'unité $f_0(e)$ telle que $f_0(E)$ soit une $\bar{Q}$-algèbre pour la restriction $\bar{Q}$ de Q_0 à $f_0(E)$. Pour tout couple $(f_0(X),f_0(X'))$ d'éléments de $f_0(E)$,

$$f_0(X)f_0(X') = -B_{1,0}(f_0(X),f_0(X'))f_0(e)+B_{1,0}(f_0(X),f_0(e))f_0(X')+B_{1,0}(f_0(X'),f_0(e))f_0(X)$$

où $B_{1,0}$ est l'extension de la forme bilinéaire B_1 à E_0.

On pose pour tout couple (X,X') d'éléments de E

$$XX' = - B_1(X,X')e + B_1(X,e)X' + B_1(X',e)X$$

On voit immédiatement que pour cette multiplication, E est muni d'une structure d'algèbre d'unité e telle que E soit une Q-algèbre donc à la fois une solution du problème préléminaire 3.3.5. et du problème 1.

Mais il peut exister des solutions du problème 3.3.5. qui ne sont pas des Q-algèbres.

Exemple.

$E = F \oplus T$ où F est le Z-module libre $Z\,e \oplus Z\,i$ et T le Z-module de torsion $Z/3Z$. On munit E de la forme quadratique Q définie par $Q(e) = 1$, $Q(i) = -\alpha$, $B(e,i) = 0$. On considère la multiplication définie sur E comme suit :

Sur F, c'est la multiplication définie par la structure d'algèbre quadratique d'unité e, de norme Q ; sur T, c'est la multiplication définie par la structure naturelle de corps de $Z/3Z$. Pour tout $X \in F$ et tout $Y \in T$ on pose $XY = YX = \frac{B(X,e)}{2} Y$, pour X et $X' \in F$, Y et $Y' \in T$ on pose
$(X + Y)(X' + Y') = XX' + YX' + XY' + YY'$.

Avec cette multiplication, E est muni d'une structure d'algèbre d'unité e solution du problème 3.3.5. qui n'est pas une Q-algèbre. (En effet, pour tout élément Y de $T - \{0\}$, $Y^2 \neq 0$ donc $Y^2 \neq -Q(Y)e + B(Y,e)Y$).

On déduit de la preuve de la proposition 3.3.6. le théorème suivant :

Théorème 3.3.7.-

Soit (E,Q) un module quadratique de rang 2 sur l'anneau intègre A vérifiant la propriété (1.2.10)'.

(1.2.10)' | Il existe une forme bilinéaire B_1 telle que, pour tout élément X de E, $Q(X) = B_1(X,X)$.

Pour qu'on puisse munir E d'une structure de Q-algèbre, autrement dit

pour qu'il existe une solution du problème 1, il faut et il suffit que la forme Q représente 1.

Pour toute algèbre solution d'unité e, $Q(e) = 1$. Inversement, à tout élément e de E tel que $Q(e) = 1$ correspond au moins une solution d'unité e.

Remarque.

On n'a pas en général unicité. Il peut exister plusieurs Q-algèbres solutions d'unité e. On donnera un exemple plus loin.

Propriétés des solutions du problème 1.

Proposition 3.3.8.-

Soit (E,Q) un module quadratique de rang 2 sur l'anneau intègre A vérifiant la propriété (1.2.10)'. Une Q-algèbre E_e solution du problème 1 n'est pas nécessairement associative, elle n'est pas nécessairement commutative.

Exemple 1.

On reprend le module quadratique précédent. $A = \mathbb{Z}$, $E = F \oplus T$ avec $F = \mathbb{Z}\, e \oplus \mathbb{Z}\, i$ et $T = \mathbb{Z}/3\mathbb{Z}$ $Q(e) = 1$ $B(e,i) = 0$ $Q(i) = -\alpha$ avec $\alpha \not\equiv 0 \mod 3$. On munit E de la structure d'algèbre E_e^1 d'unité e dont la multiplication est définie par

$$XX' = -B_1(X,X')e + B_1(X,e)X' + B_1(X',e)X \quad \text{avec} \quad B_1 = \frac{1}{2}B .$$

Soient X et X' deux éléments de F, Y un élément de T,

$$X = xe + yi \quad , \quad X' = x'e + y'i \quad (x,y,x',y' \in \mathbb{Z})$$

$$(XX')Y = \left[-B_1(X,X') + 2B_1(X,e)B_1(X',e)\right]Y \qquad X(X'Y) = B_1(X,e)B_1(X',e)Y$$

d'où $(XX')Y - X(X'Y) = \alpha\, yy'Y$. Il suffit de choisir $Y \not\equiv 0$ et y et $y' \not\equiv 0 \mod 3$ pour obtenir $(XX')Y - X(X'Y) \neq 0$. Donc E_e^1 n'est pas associative. E_e^1 est une Q-algèbre commutative non associative.

Exemple 2.

On reprend le $\mathbb{Z}$-module quadratique précédent avec α quelconque. On munit E de la structure d'algèbre E_e^2 d'unité e dont la multiplication est définie comme suit :

Sur F, c'est la multiplication définie par la structure d'algèbre quadratique d'unité e, de norme Q. Pour tout élément Y de T, on pose $eY = Ye = Y$, $iY = -Yi = Y$ et pour tout couple (Y,Y') d'éléments de T, on pose $YY' = Y'Y = 0$.

Il est immédiat que E_e^2 n'est pas commutative. C'est une Q-algèbre. En effet, pour tout élément $X + Y$ de E, $(X = xe + yi \in F , y \in T)$ $(X + Y)^2 = X^2 + XY + YX + Y^2 = X^2 + 2xY = - Q(X)e + B(X,e)X + 2xY$ ou encore, puisque $Q(Y) = B(X,Y) = B(Y,e) = B(i,e) = 0$, $(X+Y)^2 = -Q(X+Y)e + B(X+Y,e)(X+Y)$.

Remarque.

Pour le $\mathbb{Z}$-module précédent, il existe au moins deux Q-algèbres solutions du problème 1 d'unité e. Une Q-algèbre commutative E_e^1 et une Q-algèbre non commutative E_e^2.

Proposition 3.3.9.-

Soit (E,Q) un module quadratique de rang 2 sur A muni d'une structure de Q-algèbre. La forme Q est multiplicative sur E.

En effet, l'extension Q_0 de Q à E_0 est multiplicative sur l'algèbre quadratique obtenue par extension des scalaires à A_0 donc pour tout couple (X,X') d'éléments de E

$$Q(XX') = Q_0(f_0(XX')) = Q_0(f_0(X)f_0(X')) = Q_0(f_0(X))Q_0(f_0(X')) = Q(X)Q(X').$$

Remarque.

Cette propriété est vraie en particulier pour les solutions du problème 1, mais elle reste vraie pour les solutions du problème préliminaire 3.3.5. qui ne sont

pas des Q-algèbres.

Soit (E,Q) un module quadratique de rang 2 vérifiant la propriété (1.2.10)'. A tout élément e de E tel que Q(e) = 1, on a associé une Q-algèbre d'unité e dont la multiplication est définie par

$$XX' = - B_1(X,X')e + B_1(X,e)X' + B_1(X',e)X \qquad (1)$$

On désigne par $\mathcal{E}$ l'ensemble de ces solutions particulières du problème 1. On vérifie facilement que le théorème d'existence et d'unicité (Th. 3.3.3.) reste vrai à condition de se restreindre à la famille $\mathcal{E}$ des solutions du problème 1 qui vérifient (1). Il en est de même pour la caractérisation des isomorphismes d'une algèbre $E_e \in \mathcal{E}$ sur une algèbre $E_{e'} \in \mathcal{E}$.

Une algèbre $E_e \in \mathcal{E}$ est une Q-algèbre commutative. De telles algèbres seront étudiées dans le chapitre suivant. Les propriétés particulières des éléments de $\mathcal{E}$ seront données dans ce chapitre. On montrera en particulier que lorsqu'une algèbre $E_e \in \mathcal{E}$ possède des idempotents non triviaux, elle est la somme directe d'un module libre de rang 2 et d'un module de torsion.

CHAPITRE IV

G-ALGEBRES GENERALES

---

§ 1 - *Propriétés préliminaires.*

On ne suppose plus A intègre. D'après la définition 0.1.2. une Q-algèbre sur A est une A-algèbre E d'unité e munie d'une forme quadratique Q telle que $Q(e) = 1$ et telle que pour tout élément X de E.

$$X^2 = -Q(X)\, e + B(X,e)\, X$$

où B est la forme bilinéaire associée à Q.

On peut trouver une Q-algèbre E munie d'une forme quadratique Q' distincte de Q telle que E soit une Q'-algèbre.

Exemple.

On suppose que A n'est pas réduit. Soit $a \in A - \{0\}$ tel que $a^2 = 0$ et soit F une algèbre quadratique d'unité e, de base (e,j), de norme Q telle que $Q(j) = -\alpha$, $B(e,j) = 2$. On prend pour algèbre E la sous A-algèbre monogène de F engendrée par aj. (alors $E = Ae \oplus A\,aj$). E est une Q-algèbre pour la restriction de Q à E. On munit E de la forme quadratique Q' définie par $Q'(e) = 1$ $Q'(aj) = 0$ et $B'(aj,e) = 3a$. Pour tout élément $xe + yaj$ de E $(x,y \in A)$, $X^2 = -Q(X)\, e + B(X,e)\, X = -(x^2+2xya)\, e + (2x+2ay)\,(xe+yaj)$ et puisque $a^2 = 0$ $X^2 = -(x^2+3axy)\, e + (2x+3ay)\,(xe+yaj) = -Q'(X)\, e + B'(X,e)X$.

Dans cet exemple, E est à la fois une Q-algèbre et une Q'-algèbre et les formes quadratiques Q et Q' sont distinctes. Toutefois.

Proposition 4.1.1.-

Soient E une A-algèbre, Q et Q' deux formes quadratiques définies sur E telles que E soit à la fois une Q-algèbre et une Q'-algèbre. Lorsque

l'une des deux propriétés 1 et 2 ci-dessous est vérifiée, $Q = Q'$.

1) E possède une base contenant l'unité e.

2) 2 est régulier dans A et A est réduit.

Preuve.

1) Soit $(e_i)_{i\in I}$ une base de E contenant l'unité e. Alors $Q(e) = Q'(e) = 1$. Pour tout élément e_i de la base distinct de e $e_i^2 = -Q(e_i)\, e + B(e_i,e)\, e_i = -Q'(e_i)\, e + B'(e_i,e)\, e_i$ donc $Q(e_i) = Q'(e_i)$, $B(e_i,e) = B'(e_i,e)$.

Pour tout couple (e_i,e_j) d'éléments de la base distincts de e,

$$Q(e_i+e_j)^2 = -Q(e_i+e_j)\, e + B(e_i+e_j,e)\, (e_i+e_j)$$
$$Q(e_i,e_j)^2 = -Q'(e_i+e_j)\, e + B'(e_i+e_j,e)\, (e_i+e_j)$$

d'où compte tenu de $B(e_i,e) = B'(e_i,e)$ et de $B(e_j,e) = B'(e_j,e)$ $B(e_i,e_j) = B'(e_i,e_j)$. Donc $Q(X) = Q'(X)$ pour tout élément X de E.

2) On suppose que 2 est régulier dans A et que A est réduit.

Pour tout élément X de E, $X^2 = -Q(X)\, e + B(X,e)\, X$ et $X^2 = -Q'(X)\, e + B'(X,e)\, X$. Donc

$$\left[Q(X) - Q'(X)\right] e = \left[B(X,e) - B'(X,e)\right] X$$

on en déduit, compte tenu de $B(e,e) = B'(e,e) = 2$,

$$2\left[Q(X) - Q'(X)\right] = \left[B(X,e) - B'(X,e)\right] B(X,e)$$

$$2\left[Q(X) - Q'(X)\right] = \left[B(X,e) - B'(X,e)\right] B'(X,e)$$

d'où $\left[B(X,e) - B'(X,e)\right]^2 = 0$ et puisque A est réduit et 2 régulier dans A, $B(X,e) = B'(X,e)$ et $Q(X) = Q'(X)$.

Remarque.

Les algèbres de quaternions et les algèbres de Cayley sont des Q-algèbres et vérifient les conditions de la proposition 4.1.1. Chacune d'elles ne peut être une Q-algèbre que pour une seule forme Q.

Lorsque 2 est régulier, on a la généralisation suivante de la proposition 3.3.4. du chapitre précédent.

Proposition 4.1.2.-

Soit E une A-algèbre d'unité e. On suppose que 2 est régulier dans A et que l'une des conditions 1 et 2 ci-dessous est vérifiée.

1) E possède une base contenant l'unité e.

2) A est intègre, E de rang ≥ 2

Alors, pour qu'il existe une forme quadratique Q définie sur E telle que E soit une Q-algèbre, il faut et il suffit que tout élément X de E vérifie une équation de la forme

$$X^2 = \alpha(X)\, e + \beta(X)\, X \ , \ (\alpha(X), \beta(X) \in A) \ .$$

Preuve.

- Lorsque E est une Q-algèbre, tout élément X de E vérifie l'équation $X^2 = -Q(X)\, e + B(X,e)\, X$ qui est de la forme indiquée.

- On suppose maintenant que tout élément X de E vérifie une équation de la forme $X^2 = \alpha(X)\, e + \beta(X)\, X$, $(\alpha(X), \beta(X) \in A)$. On va montrer que lorsque de plus l'une des conditions 1 et 2 est vérifiée, il existe une forme Q telle que E soit une Q-algèbre.

1) On suppose qu'il existe une base $(e_i)_{i \in I}$ de E contenant e.

Soit $e_{i_o} = e$. On pose $\alpha_{i_o} = -1$ $\beta_{i_o} = 2$ et pour tout $i \in I - \{i_o\}$, on pose $\alpha_i = \alpha(e_i)$ et $\beta_i = \beta(e_i)$. Pour tout couple (i,j) d'éléments de i,

$i \neq j$, $i \neq i_o$, $j \neq i_o$, on pose $\alpha(e_i+e_j) = \gamma_{ij}$ et $\beta(e_i+e_j) = \delta_{ij}$.

Alors $e_ie_j+e_je_i = (e_i+e_j)^2-e_i^2-e_j^2 = (\gamma_{ij}-\alpha_i-\alpha_j)e+(\delta_{ij}-\beta_i)e_i+(\delta_{ij}-\beta_j)e_j$ et quels que soient les éléments a, a_i, aj de A

$$1) \quad (ae+a_ie_i+a_je_j)^2 = ke + \ell(ae+a_ie_i+a_je_j)$$

où on a posé $k = \alpha(ae+a_ie_i+a_je_j)$ et $\ell = \beta(ae+a_ie_i+a_je_j)$

k et ℓ dépendent de i, j, a, a_i, a_j.

On développe le premier membre de (1)

$$a^2e + a_i^2(\alpha_ie-\beta_ie_i) + a_j^2(\alpha_je+\beta_je_j) + 2aa_ie_i + 2aa_je_j +$$

$$+ a_ia_j\left[(\gamma_{ij}-\alpha_i-\alpha_j)e + (\delta_{ij}-\beta_i)e_i + (\delta_{ij}-\beta_j)e_j\right] = ke + \ell(ae+a_ie_i+a_je_j)$$

Puisque e, e_i, e_j sont des éléments de base distincts, (1) implique

$$\left[2a + (\delta_{ij}-\beta_i)a_j + \beta_ia_i\right]a_i = a_i\ell$$

$$\left[2a + (\delta_{ij}-\beta_j)a_i + \beta_ja_j\right]a_j = a_j\ell$$

en particulier lorsque $a_i = 1$, $a_j = -1$

$$2a - \delta_{ij} + \beta_i + \beta_j = 2a + \delta_{ij} - \beta_i - \beta_j$$

et puisque 2 est régulier, $\delta_{ij} = \beta_i + \beta_j$

On considère maintenant la forme quadratique Q définie comme suit sur E.

Pour tout $i \in I$, on pose $Q(e_i) = -\alpha_i$ et $B(e_i,e) = \beta_i$. Pour tout couple (i,j) d'éléments de I tels que $i \neq j$, $i \neq i_o$, $j \neq i_o$, on pose $B(e_i,e_j) = \alpha_i + \alpha_j - \gamma_{ij}$.

Alors, pour tout élément X de E, $X^2 = -Q(X)\,e + B(X,e)\,X$. En effet : Soit $X = ae + \sum_{i \in L} a_ie_i$, $(a, a_i \in A$, L fini inclus dans I, $i_o \notin L)$.

E est le module libre de base (e,e_1,e_2) muni de la structure d'algèbre d'unité e telle que $e_1^2 = 0$, $e_2^2 = 0$, $e_1e_2 = e_1$, $e_2e_1 = e_2$. Alors $(e+e_1)^2 = e$, $(e+e_2)^2 = e$, $(e+e_1+e_2)^2 = e + e_1 + e_2$, $(e_1+e_2)^2 = e_1 + e_2$. Tout élément X de E vérifie donc une équation de la forme $X^2 = \alpha(X)\, e + \beta(X)\, X$, $(\alpha(X), \beta(X) \in A)$ mais il n'existe pas de forme quadratique Q pour laquelle E est une Q-algèbre. En effet :

$e_1^2 = 0$ et $e_2^2 = 0$ impliquent $B(e_1,e) = B(e_2,e) = 0$ et $(e_1+e_2)^2 = e_1 + e_2$ implique $B(e_1+e_2,e) = 1$ ce qui est incompatible avec la bilinéarité de B.

Propriétés d'une Q-algèbre (commutative ou non)

Une Q-algèbre n'est pas nécessairement associative (cf. ch. III) cependant :

Proposition 4.1.3.-

Soit E une Q-algèbre. Chaque sous-algèbre monogène de E est associative et commutative.

Preuve. (voir aussi [1])

Soit E une Q-algèbre et soit X un élément de E. Alors $X^2 = -Q(X)\, e + B(X,e)\, X$. On pose $Q(X) = -a$ $B(X,e) = b$. $X^2 = ae + b\, X$, X^2 est de la forme $x_2\, e + y_2\, X$ $X^2X = a\, y_2\, e + (x_2+by_2)\, X = X.X^2$

On note X^3 cette valeur commune qui est de la forme $x_3\, e + y_3\, X$

- Hypothèse de récurrence. On suppose que

1) X^k est défini pour $1 \leq k \leq n$, c'est-à-dire que pour k fixé tous les produits formés avec k éléments égaux à X ont la même valeur. On note X^k cette valeur commune.

2) Pour tout entier k, $(1 \leq k \leq n)$, il existe deux éléments x_k et y_k de A tels que ,

$$\forall\, k \leq n\ ,\ X^k = x_k e + y_k X$$

$$\forall\, k < n\ ,\ X^{k+1} = a\, y_k e + (x_k + b\, y_k)\, X$$

- Alors X^{n+1} est défini et l'hypothèse 2 est vérifiée pour $1 \leq k \leq n + 1$. En effet :

Pour montrer que X^{n+1} est défini, il suffit de montrer, compte tenu de l'hypothèse de récurrence, que pour tous entiers r et p tels que $1 \leq r \leq n - 1$, $1 \leq p \leq n - 1$ et $r + p = n$, $X^r\, X^{n+1} = X^{r+1}\, X^p$.

- Puisque $p < n$ et $r < n$

$$X^{p+1} = a\, y_p\, e + (x_p + b\, y_p)\, X\ ,\ X^{r+1} = a\, y_r\, e + (x_r + b\, y_r)\, X$$

$$X^r\, X^{p+1} = \left[x_r e + y_r X\right] \cdot \left[a\, y_p\, e + (x_p + b\, y_p)\, X\right] = X^{p+1}\, X^r \quad \text{(immédiat)}$$

On obtient après réduction, compte tenu de $X^2 = ae + b\, X$

$$X^r\, X^{p+1} = a\left[x_r\, y_p + y_r\, x_p + b\, y_r\, y_p\right] e + \left[(a + b^2)\, y_r\, y_p + b(y_r\, x_p + x_r\, y_p) + x_r\, x_p\right] X$$

Comme cette expression est symétrique en r et p

$X^r\, X^{p+1} = X^p\, X^{r+1}$ et compte tenu de $X^p\, X^{r+1} = X^{r+1}\, X^p$, $X^r\, X^{p+1} = X^{r+1}\, X^p$

Donc X^{n+1} est défini et en particulier ,

$$X^{n+1} = XX^n = a\, y_n\, e + (x_n + b\, y_n)\, X$$

ce qui permet de définir x_{n+1} et y_{n+1} tels que l'hypothèse 2 soit vérifiée à l'ordre $n + 1$.

Les hypothèses de récurrence étant vérifiées pour $n \leq 3$, on en déduit que X^n est défini pour tout $n \in \mathbb{N}$.

De plus, puisque pour tout couple (p,q) d'entiers ≥ 0 $X^p X^q = X^q X^p = X^{p+q}$, la sous-algèbre engendrée par X est commutative.

Proposition 4.1.4.-

Soit E une Q-algèbre. La forme quadratique Q est multiplicative sur chaque sous-algèbre monogène de E.

Preuve.

Soit X un élément de E. D'après la proposition 4.1.3, la sous-algèbre engendrée par X est associative et commutative. On peut donc la noter $A[X]$. Puisque $X^2 = -Q(X)\, e + B(X,e)\, X$, il est immédiat que $A[X] = Ae + AX$.

Soient $xe + y X$ et $x'e + y'X$ deux éléments de $A[X]$. On pose $Q(X) = -a$, $B(X,e) = b$. Alors

$$Q(xe + y X)\, Q(x'e + y'X) = (x^2 - ay^2 + b\, xy)\, (x'^2 - ay'^2 + b\, x'y')$$

$$(xe + y X)\, (x'e + y'X) = (xx' + a\, yy')\, e + (xy' + x'y + b\, yy')\, X$$

On constate après réductions que

$$Q[(xe + y X)\, (x'e + y'X)] = Q(xe + y X)\, Q(x'e + y'X)$$

Conséquence.

$$\forall X \in E\ ,\ \forall n \in \mathbb{N}\ ,\ Q(X^n) = (Q(X))^n\ .$$

Corollaire 1.

Soit E une Q-algèbre sur A. Pour qu'un élément X de E soit inversible dans $A[X]$, il faut et il suffit que $Q(X)$ soit inversible dans A.

La preuve est immédiate, analogue à la preuve faite pour les algèbres quadratiques (Prop. 1.2.1. cor. 1).

Corollaire 2.

On suppose que A est réduit. Soit E une Q-algèbre sur A d'unité e. L'ensemble des éléments nilpotents de E est l'ensemble des éléments X de E tels que $Q(X) = B(X,e) = 0$. C'est donc l'ensemble des éléments de carré nul.

La preuve est analogue à la preuve du début de la proposition 1.2.4. Mais ici l'ensemble des éléments nilpotents n'est pas nécessairement égal au noyau K_1 du module quadratique (E,Q). L'inclusion de K_1 dans cet ensemble peut être stricte. (On peut prendre par exemple un module libre E de base (e, X, Y) avec $Q(X) = B(X,e) = 0$ et $B(X,Y) \neq 0$).

Autre application de la proposition 4.1.4 :

Recherche des idempotents d'une Q-algèbre.

Soit E une Q-algèbre d'unité e. Pour tout idempotent non trivial a de A, ae est un idempotent non trivial de E. Pour exclure ces idempotents, on suppose dans ce qui suit que A ne possède pas d'idempotents non triviaux.

Les idempotents de E sont les solutions de l'équation $Y^2 = Y$ c'est-à-dire de

$$(2) \qquad -Q(Y)\,e + B(Y, e)\,Y = Y$$

Pour toute solution Y de (2), $[Q(Y)]^2 = Q(Y^2) = Q(Y)$, donc $Q(Y)$ est un idempotent de A. Compte tenu de l'hypothèse faite sur A, $Q(Y) = 0$ ou $Q(Y) = 1$.

- Lorsque $Q(Y) = 1$, (2) s'écrit $Y(B(Y, e) - 1) = e$

ce qui implique $(B(Y,e) - 1)^2 = Q(e) = 1$ et $B(Y, e)\,(B(Y, e) - 1) = B(e, e) = 2$ on en déduit $B(Y,e) = 2$ donc $Y = e$.

- Lorsque $Q(Y) = 0$, (2) s'écrit $Y(B(Y, e) - 1) = 0$

ce qui implique $B(Y,e)\,(B(Y, e) - 1) = 0$ et puisque A ne possède pas d'idempotents non triviaux, $B(Y,e) = 1$ ou $B(Y, e) = 0$. Lorsque $B(Y,e) = 0$, $Y = 0$.

Lorsque $B(Y,e) = 1$, Y est un idempotent non trivial de E. En définitive.

Proposition 4.1.5.-

Soit E une Q-algèbre sur A d'unité e. On suppose que A ne possède pas d'idempotents non triviaux. Alors, pour qu'un élément Y de E soit un idempotent non trivial, il faut et il suffit que $Q(Y) = 0$ et $B(Y, e) = 1$.

Dans le paragraphe suivant, on étudie une famille de Q-algèbres commutatives.

§ 2 - *Q-algèbres commutatives associées à une forme bilinéaire symétrique.*

Hypothèses et définitions 4.2.1.

Soient E un A-module et B_1 une forme bilinéaire symétrique définie sur E^2. A tout élément e de E tel que $B_1(e, e) = 1$, on peut associer la structure d'algèbre sur E dont la multiplication est définie pour tout couple (X,X') d'éléments de E par

$$(1)\quad XX' = -B_1(X,X')\, e + B_1(X,e)\, X' + B_1(X',e)\, X$$

Pour tout élément X de E, on pose $Q(X) = B_1(X,X)$, alors $2\,B_1$ est la forme bilinéaire associée à la forme quadratique Q et E est une Q-algèbre d'unité e. On pose $B = 2\,B_1$.

Lorsque E est muni de cette structure, on dit que E est la Q-algèbre d'unité e associée à la forme B_1.

Lorsque 2 est régulier, la donnée de la forme Q détermine B_1.

Lorsque 2 est inversible dans A, toutes les Q-algèbres commutatives sur A sont de ce type.

Les solutions du problème 1 (chap. I et chap. III § 1) pour les modules quadratiques vérifiant la propriété (1.2.10)' sont aussi des algèbres de ce type.

Il en est de même pour la famille particulière $\mathcal{E}$ des solutions du problème 1 du § 3 chap. III.

1 - Propriétés complémentaires.

Toute Q-algèbre associée à une forme bilinéaire symétrique est de puissances associatives (prop. 4.1.3). De plus :

Proposition 4.2.2.-

Toute Q-algèbre associée à une forme bilinéaire symétrique B_1 est une algèbre de Jordan commutative.

En effet, pour tout couple (X,Y) d'éléments de E

$$X^2(XY) = \left[B_1(X,X)\, B_1(X,Y) - 2\, B_1(X,X)\, B_1(X,e)\, B_1(Y,e) - 2\, B_1^2(X,e)\, B_1(X,Y)\right] e$$

$$+ \left[- B_1(X,X)\, B_1(Y,e) + 6\, B_1^2(X,e)\, B_1(Y,e) - 2\, B_1(X,Y)\, B_1(X,e)\right] X$$

$$+ \left[- B_1(X,X)\, B_1(X,e) + 2\, B_1^3(X,e)\right] Y$$

$$= (X^2\, Y)\, X$$

Proposition 4.2.3.-

Soit E une Q-algèbre d'unité e associée à une forme bilinéaire symétrique B_1. La forme linéaire $X \mapsto B_1(X,e)$ est associative.

En effet, quels que soient les éléments X, X', X'' de E

$$(XX')\,X''-X(X'X'')=\left[-B_1(X,e)B_1(X'X'')+B_1(X'',e)B_1(X,X')\right]e+\left[B_1(X,e)B_1(X',e)-B_1(X,X')\right]X''$$

$$+\left[-B_1(X'',e)B_1(X',e)+B_1(X'',X')\right]X$$

d'où $B_1((XX')X'',e) - B_1(X(X'X''),e) = 0$

2 - Etude d'une Q-algèbre associée à une forme bilinéaire symétrique qui possède des idempotents non triviaux.

Soit E la Q-algèbre d'unité e associée à la forme bilinéaire B_1.

On suppose que A n'a pas d'idempotents non triviaux et que E possède un idempotent non trivial Y.

Y est solution du système $(Q(Y) = 0 \ , \ 2\,B_1(Y, e) = 1)$. Donc 2 est inversible dans A.

a) Décomposition associée à un idempotent non trivial.

Proposition 4.2.4.-

On suppose que A n'a pas d'idempotents non triviaux et on désigne par E une Q-algèbre d'unité e associée à une bilinéaire symétrique B_1.

A tout idempotent non trivial Y de E, on peut associer une décomposition en somme directe de A-modules $E = E'_Y \oplus E''_Y \oplus E'''_Y$ possédant les propriétés suivantes :

1) Soit $M_Y = E'_Y \oplus E''_Y$. M_Y est une sous A-algèbre de E. C'est une algèbre quadratique de base $(Y, e - Y)$. $E' = AY$, $E'' = A(e - Y)$. M_Y est une sous-algèbre associative maximale de E.

2) Q n'est pas dégénérée sur M_Y, E'_Y et E''_Y sont des sous-modules totalement isotropes de (E,Q) et E'''_Y est l'orthogonal de M_Y dans (E,Q).

Preuve.

Pour simplifier, on néglige l'indice Y lorsque Y est fixé.

Soit Y un idempotent non trivial de E. On utilise la décomposition de Peirce des algèbres de Jordan commutatives sur un corps de caractéristique $\neq 2$ par exemple [1] .

$E = E' \oplus E'' \oplus E'''$ où

$E' = \{X \mid X \in E \text{ et } XY = X\}$, $E'' = \{X \mid X \in E \text{ et } XY = 0\}$, $E''' = \{X \mid X \in E \text{ et } 2XY = X\}$

Tout élément X de E s'écrit de façon unique sous la forme $X = X' + X'' + X'''$ avec

$$X' = 2(XY)\,Y - XY \qquad X'' = X - 3XY + 2(XY)\,Y \qquad X''' = 4XY - 4(XY)\,Y$$

Il est immédiat que cette décomposition existe aussi pour les algèbres sur un anneau commutatif unitaire dans lequel 2 est inversible.

M est une sous-algèbre de E

En effet :

Puisque Y et $e - Y$ sont des éléments de M, e appartient à M. Pour tout couple (X_1, X_2) d'éléments de M, $X_1X_2 = -B_1(X_1,X_2)e + B_1(X_1,e)X_2 + B_1(X_2,e)X_1$ donc $X_1 X_2$ appartient à M.

M est une algèbre quadratique de base $(e, e-Y)$: $E' = AY$, $E'' = A(e-Y)$

En effet : $X \in M \iff 4XY - 4(XY)\,Y = 0$

Compte tenu de $Y^2 = Y$ et de $B(Y,e) = 1$, (avec $B = 2B_1$),

$$4XY = -2B(X,Y)\,e + 2B(X,e)\,Y + 2X$$

$$4(XY)Y = -2B(X,Y)\,Y + 2B(X,e)\,Y - B(X,Y)\,e + B(X,e)\,Y + X$$

Donc :

(2) $X \in M \iff X = [B(X,e) - 2B(X,Y)]\,Y + B(X,Y)\,e$

D'autre part, e et Y sont des éléments de M linéairement indépendants. En effet :

$$(ae + bY = 0,\ a \text{ et } b \in A) \Rightarrow (B(ae + bY, e) = B(ae + bY, Y) = 0)$$

et le second membre s'écrit, compte tenu de $Q(Y) = 0$ et $B(Y,e) = 1$,

$$2a + b = a = 0 .$$

Donc $$(ae + bY = 0) \Rightarrow (a = b = 0)$$

e et Y forment donc une base de M. Il est immédiat que $(Y, e - Y)$ est aussi une base de M.

Plus particulièrement :

Soit X un élément de E', $XY = X$ implique $X = -B(X,Y)\, e + B(X,e)\, Y$ compte tenu de (2), $2B(X,Y)\,(e - Y) = 0$

Comme e et Y forment un système libre, $B(X,Y) = 0$ et $X = B(X,e)\, Y$ Puisque Y est un élément de E', $E' = AY$.

Soit X élément de E", un calcul analogue montre que $X = B(X,e)\,(e - Y)$ On en déduit de même que $E'' = A(e - Y)$.

M est une sous-algèbre associative maximale de E. En effet :

D'après ce qui précède, M est la sous-algèbre monogène engendrée par Y, elle est donc associative. D'autre part, pour tout élément X de $E - M$, $XY \neq (XY)\, Y$ et $XY = XY^2$ donc $(XY)\, Y \neq X\, Y^2$. Donc les sous-algèbres de E qui contiennent strictement M ne sont pas associatives.

E' et E" sont des sous-modules totalement isotropes de E. La restriction de Q à M n'est pas dégénérée et dans E, $E''' = M^{\perp}$

En effet :

- Puisque $E' = AY$, $E'' = A(e - Y)$ et $Q(Y) = Q(e - Y) = 0$, il est immédiat que pour tout élément X de $E' \cup E''$, $Q(X) = 0$.

- Soit X un élément de E, $X = X' + X'' + X'''$

$$X \in E''' \iff (X' = X'' = 0)$$

donc $X \in E''' \iff (XY = 2(XY)\,Y \text{ et } X = 3\,XY - 2(XY)\,Y)$

$$X \in E''' \iff X = -\,B(X,Y)\,e + B(X,e)\,Y = 0$$

(compte tenu de $Y^2 = Y$ et $B(Y,e) = 1$)

Comme e et Y sont linéairement indépendants, cette condition équivaut à $B(X,Y) = B(X,e) = 0$ et puisque (e,Y) est une base de M :

$$X \in E''' \iff X \text{ est orthogonal à } M$$

Donc $E''' = M^{\perp}$ et la restriction de Q à M n'est pas dégénérée.

Remarque 1.

$e - Y$ est un idempotent non trivial de E. La décomposition associée à $e - Y$ est obtenue en échangeant E' et E'' dans la décomposition associée à Y.

Remarque 2.

Lorsqu'on ne suppose plus que A ne possède pas d'idempotents non triviaux, la proposition 4.2.4. reste vraie, à condition d'exclure les idempotents Y de E qui ne vérifient pas les deux conditions $Q(Y) = 0$ et $B(Y,e) = 1$.

Conséquences de la proposition 4.2.4.

On suppose dans cette partie que E possède un idempotent Y tel que $Q(Y) = 0$ et $B(Y,e) = 1$ et on désigne par $E' \oplus E'' \oplus E'''$ la décomposition associée à Y selon la proposition 4.2.4.

Soit K_1 le noyau du module quadratique (E,Q), $(K_1 = \{X \in E \mid Q(X) = 0 \text{ et } \forall\, X' \in E,\ B(X,X') = 0\})$, K_1 est un sous-module de E. De plus

$$\forall\, X \in K_1\ ,\ \forall\, Z \in E \qquad 2\,XZ = B(X,e)\,Z \qquad (XZ = B_1(X,e)\,Z)$$

En particulier :

$$\forall\, X \in K_1 \,,\; 2\,XY = X$$

Donc K_1 est un idéal de E contenu dans E'''

Proposition 4.2.5.-

Soit E une Q-algèbre d'unité e associée à une forme bilinéaire B_1. On suppose que E possède un idempotent Y tel que $Q(Y) = 0$ et $2\,B_1(Y,e) = 1$. On désigne par $E' \oplus E'' \oplus E'''$ la décomposition de Peirce associée à Y selon la proposition 4.2.4. et par K_1 le noyau du module quadratique (E,Q). Les propriétés suivantes sont équivalentes.

1) $K_1 = E'''$

2) E''' est un idéal de E

3) La forme Q est multiplicative par E.

Preuve.

On sait que K_1 est un idéal de E contenu dans E'''.

1 $\Longleftrightarrow$ 2. En effet

- Lorsque $E''' = K_1$, E''' est un idéal de E.

- Pour tout couple (X_1,X_2) d'éléments de E''' , $X_1\,X_2 = -\frac{1}{2}\,B(X_1,X_2)\,e$ (car $B(X_1,e) = B(X_2,e) = 0$ puisque $E''' = M^{\perp}$). Lorsque E''' est un idéal de E, $X_1\,X_2 \in E'''$, donc $B(X_1,X_2) = 0$ (car e est libre). Puisque $E''' = M^{\perp}$, E''' est aussi l'orthogonal de E. Autrement dit, $E''' = K_1$.

2 $\Longleftrightarrow$ 3. En effet

- On suppose Q multiplicative sur E

$\forall\, X_1$ et $X_2 \in E'''$, $B(X_1,X_2) = B(2\,X_1\,Y,\, 2\,X_2\,Y) = 4\,Q(Y)\,B(X_1,X_2) = 0$

On voit comme plus haut que $E''' = K_1$

- On suppose que $E''' = K_1$.

Soient X_1 et X_2 deux éléments de E. $X_1 = Z_1 + X_1'''$, $X_2 = Z_2 + X_2'''$ avec Z_1 , $Z_2 \in M$ et X_1''' , $X_2''' \in K_1$

$$X_1 X_2 = Z_1 Z_2 + X_1'''(Z_2 + X_2''') + X_2''' Z_1$$

Dans le second membre le premier produit est un élément de M puisque M est une sous-algèbre de E, les deux autres produits sont des éléments de K_1 puisque K_1 est un idéal.

Donc $Q(X_1 X_2) = Q(Z_1 Z_2) = Q(Z_1) Q(Z_2)$, puisque Q est multiplicative sur l'algèbre quadratique M. Comme de plus $Q(X_1) = Q(Z_1)$ et $Q(X_2) = Q(Z_2)$, $Q(X_1 X_2) = Q(X_1) Q(X_2)$.

Corollaire 1.

Soit E une Q-algèbre associée à une forme bilinéaire symétrique qui possède un idempotent Y tel que $Q(Y) = 0$ et $B(Y,e) = 1$. On suppose que Q n'est pas dégénérée sur E. Alors, pour que Q soit multiplicative sur E, il faut et il suffit que E soit libre de rang 2.

Preuve.

Lorsque Q n'est pas dégénérée, $K_1 = (0)$. Lorsque de plus Q est multiplicative $(0) = K_1 = E'''$ (prop. 4.2.5). Donc E est libre de rang 2 (prop. 4.2.4.).

Inversement, lorsque E est une algèbre quadratique, Q est multiplicative sur E (chap. I).

Corollaire 2.

On suppose que A est intègre. Soit (E,Q) un A-module quadratique de rang 2 qui vérifie la propriété (1.2.10)'.

Toute solution du problème 1 (Th. 3.3.5) qui appartient à $\mathcal{E}$ (c'est-à-dire qui est une Q-algèbre associée à une forme bilinéaire B_1) et qui possède un idempotent non trivial est la somme directe d'un module libre de rang 2 et du

son sous-module de torsion T.

On a déjà vu que Q est multiplicative sur une telle solution (prop.3.3.9). Donc $K_1 = E'''$ est de rang zéro $T = K_1 = E'''$

Remarque.

Il peut arriver qu'une solution du problème 1 ne possède pas d'idempotents non triviaux et admette une décomposition de la forme $M \oplus T$ (ex. 1 du § 3, chap. III).

Corollaire 3.

On suppose que A est intègre et que 2 est inversible dans A. Soit E un module sans torsion de rang 2 sur A. Pour que E soit libre, il faut et il suffit qu'il existe une forme quadratique Q définie sur E et deux éléments e et Y de E tels que $Q(e) = 1$, $Q(Y) = 0$ et $B(Y,e) = 1$. (e, Y) est alors une base de E.

Cette condition est nécessaire. En effet, on peut toujours munir un module de base (e,Y) de la forme quadratique Q définie par $Q(e) = 1$, $Q(Y) = 0$ et $B(Y,e) = 1$.

Elle est suffisante. En effet, la Q-algèbre d'unité e associée à la forme bilinéaire $\frac{1}{2}B$ est une solution du problème 1 qui possède un idempotent non trivial Y (prop. 4.1.5). Elle admet donc la décomposition $A\,Y \oplus A(e - Y) \oplus T$ (cor. 2) et ici $T = (0)$. En particulier le couple (e, Y) est une base de E.

b) Quelques propriétés des idempotents et des sous-algèbres associées.

On suppose ici que A ne possède pas d'idempotents non triviaux.

Soit E une Q-algèbre d'unité e associée à une forme bilinéaire symétrique B_1 qui possède un idempotent non trivial Y. Soit M la sous-algèbre libre associée à Y par la proposition 4.2.4. les seuls idempotents non triviaux de M sont Y et e - Y. En effet, soit Y' un idempotent non trivial de M ,

$Y' = a\,Y + b\,(e - Y)$, $(a, b \in A)$ $Q(Y') = ab = 0$ $B(Y',e) = a + b = 1$.

Puisque A n'a pas d'idempotents non triviaux, $a = 0$ ou 1 $b = 1 - a$. Donc $Y' = Y$ ou $Y' = e - Y$.

Soient M et M_1 les sous-algèbres libres associées à deux idempotents Y et Y_1 de E. Ae est contenu dans $M \cap M_1$. De plus, lorsque A est intègre $M \cap M_1$ est distinct de Ae si et seulement si $Y - Y_1$ ou $Y - (e - Y_1)$ appartient au sous-module de torsion T de E. En effet :

Soit X un élément de $M \cap M_1$, $X = ae + b\,Y = a_1 e + b_1\,Y$, $(a, b, a_1, b_1 \in A)$ donc $(a - a_1)\,e = b_1\,Y_1 - b\,Y$. On en déduit successivement en transformant par $B(.,e)$, $B(.,Y)$, $B(.,Y_1)$, compte tenu de $B(Y,e) = B(Y_1,e) = 1$ et $Q(Y) = Q(Y_1) = 0$,

$$2(a - a_1) = b_1 - b\,,\quad a - a_1 = b_1\,B(Y_1,Y)\,,\quad a - a_1 = -\,b\,B(Y_1,Y)$$

ce qui implique $(b - b_1)\,(1 - B(Y_1,Y)) = 0$

- <u>si $b = b_1$</u>, $a = a_1$ et puisque $(a - a_1)\,e = b(Y_1 - Y)$, $b = b_1 = 0$ ou $Y_1 - Y \in T$

- <u>si $b \neq b_1$</u>, $a \neq a_1$, $B(Y_1,Y) = 1$, $b + b_1 = 0$ $(a - a_1)\,(e - Y - Y_1) = 0$. Donc $e - Y - Y_1 \in T$.

Inversement lorsque $Y_1 - Y$ appartient à T, il existe $b \in A - \{0\}$ tel que $b(Y_1 - Y) = 0$. Alors, $\forall\, a \in A$, $ae + b\,Y = ae + b\,Y_1$. Donc $ae + b\,Y$ appartient à $M \cap M_1 - Ae$.

En particulier, lorsque E est sans torsion, ou bien $M \cap M_1 = Ae$ ou bien $M = M_1$.

3 - <u>Etude des automorphismes d'une Q-algèbre associée à une forme bilinéaire symétrique B_1</u>.

Dans cette partie on suppose que 2 est régulier. B_1 est alors déterminée par la donnée de la forme Q associée.

Proposition 4.2.6.-

On suppose que 2 est régulier dans A. Soit E une Q-algèbre sur A d'unité e associée à une forme bilinéaire symétrique B_1.

Le groupe des automorphismes de l'algèbre E contient le groupe des transformations orthogonales de (E,Q) qui laissent e invariant. Ces deux groupes peuvent être distincts.

Toutefois, lorsque l'une des conditions a,b,c ci-dessous est vérifiée les deux groupes coïncident.

a) A est réduit

b) E possède une base contenant e

c) E possède des idempotents non triviaux, A n'en possède pas.

Preuve.

Toute transformation orthogonale qui laisse e invariant est un automorphisme de l'algèbre E. En effet, la multiplication de l'algèbre E est déterminée par la donnée de e et de la forme Q.

Exemple d'inclusion stricte.

On suppose que A n'est pas réduit et que 2 est régulier. On reprend l'exemple du § 1 p. 84 . Soit $a \in A - \{0\}$ tel que $a^2 = 0$ et soit F l'algèbre quadratique d'unité e, de base (e,j) de norme Q telle que $Q(j) = -\alpha$, $B(e,j) = 2$. On prend pour E la sous-algèbre monogène de F engendrée par aj. La Q-algèbre E est associée à e et à la forme bilinéaire $\frac{B}{2}$. L'automorphisme τ du A-module F défini par $\tau(e) = e$, $\tau(j) = e + j$ induit un automorphisme τ' de E compatible avec la multiplication de E. En effet :

$$\tau'(e) = e \qquad \tau'(e\,aj) = \tau'(e)\,\tau'(aj)$$

$$\tau'((aj)^2) = a^2 \quad \tau'(j^2) = 0 = a^2(\tau'(j))^2 = (\tau'(aj))^2 \quad \text{puisque } a^2 = 0$$

Mais τ' n'est pas une transformation orthogonale de (E,Q). En effet : $B(aj,e) = 2a$ et $B(\tau'(aj), \tau'(e)) = 4a$.

(τ n'est pas compatible avec la multiplication de F).

Etude des cas a,b,c.

Soit σ un automorphisme de l'algèbre E, alors, pour tout élément X de E,

$$(3)\quad 0 = \sigma(X^2) - (\sigma(X))^2 = -\left[Q(X) - Q(\sigma(X))\right] e + \left[B(X,e) - B(\sigma(X),e)\right] \sigma(X)$$

et pour tout couple (X,X') d'éléments de E

$$(4)\quad 0 = 2\,\sigma(XX') - 2\,\sigma(X)\,\sigma(X') = -\left[B(XX')-B(\sigma(X),\sigma(X'))\right]e + \left[B(X,e)-B(\sigma(X),e)\right]\sigma(X') + \left[B(X',e)-B(\sigma(X'),e)\right] \sigma(X)$$

a) On suppose que A est réduit.

De (3) on déduit en appliquant σ^{-1} aux deux membres

$$(3')\qquad -\left[Q(X) - Q(\sigma(X))\right] e + \left[B(X,e) - B(\sigma(X), e)\right]X = 0$$

puis de (3) et (3')

$$-2\left[Q(X) - Q(\sigma(X))\right] + \left[B(X,e) - B(\sigma(X),e)\right] B(\sigma(X),e) = 0$$

$$-2\left[Q(X) - Q(\sigma(X))\right] + \left[B(X,e) - B(\sigma(X),e)\right] B(X,e) = 0$$

d'où $\left[B(X,e) - B(\sigma(X),e)\right]^2 = 0$ et puisque A est réduit et 2 régulier $B(X,e) = B(\sigma(X),e)$ et $Q(X) = Q(\sigma(X))$

Donc σ est une transformation orthogonale de (E,Q)

b) On suppose que E possède une base contenant e

Lorsque e, X et X' sont linéairement indépendants (4) implique

$$B(X,X') - B(\sigma(X), \sigma(X')) = B(X,e) - B(\sigma(X),e) = B(X',e) - B(\sigma(X'),e) = 0$$

et lorsque e et X sont linéairement indépendants (3) implique

$$Q(X) - Q(\sigma(X)) = B(X,e) - B(\sigma(X),e) = 0$$

Donc, lorsque E possède une base $(e_i)_{i\in I}$ contenant e, on a $\forall$ i et j $\in$ E, $B(e_i,e_j) = B(\sigma(e_i), \sigma(e_j))$

d'où

$\forall$ X et X' $\in$ E , $B(X,X') = B(\sigma(X), \sigma(X'))$ et $\forall$ X $\in$ E , $Q(X) = Q(\sigma(X))$

c) On suppose que E possède un idempotent non trivial, que A n'en possède pas.

Soit $M_Y \oplus E'''_Y$ la décomposition associée à l'idempotent non trivial Y selon la proposition 4.2.4. On voit facilement que $\sigma(Y)$ est un idempotent non trivial de E et que $\sigma(M_Y) \oplus \sigma(E'''_Y)$ est la décomposition associée à $\sigma(Y)$.

Soient $X_1 = m_1 + Z_1$, $X_2 = m_2 + Z_2$ $(m_1, m_2 \in M_Y, Z_1, Z_2 \in E'''_Y)$

$B(X_1,X_2) = B(m_1,m_2) + B(Z_1,Z_2)$ car M_Y et E'''_Y sont orthogonaux.

De même, $B(\sigma(X_1), \sigma(X_2)) = B(\sigma(m_1), \sigma(m_2)) + B(\sigma(Z_1), \sigma(Z_2))$.

Y et $\sigma(Y)$ sont des idempotents non triviaux de E, donc

$$Q(Y) = Q(\sigma(Y)) = 0 \quad \text{et} \quad B(Y,e) = B(\sigma(Y)),e) = 1$$

Par suite, $B(m_1, m_2) = B(\sigma(m_1), \sigma(m_2))$

D'autre part, pour tout couple (Z_1,Z_2) d'éléments de E'''_Y ,

$$2 Z_1 Z_2 = -B(Z_1, Z_2)\, e$$

donc $2\, \sigma(Z_1)\, \sigma(Z_2) = - B(Z_1,Z_2)\, e$

Puisque dans $E'''_{\sigma(Y)}$, $2\, \sigma(Z_1)\, \sigma(Z_2) = - B(\sigma(Z_1), \sigma(Z_2))\, e$

on a aussi $B(Z_1,Z_2) = B(\sigma(Z_1),\sigma(Z_2))$ (e est libre puisque $B_1(e,e) = 1$)

Donc, $\forall X_1$ et $X_2 \in E$, $B(X_1,X_2) = B(\sigma(X_1), \sigma(X_2))$.

Remarque 1.

Les deux groupes peuvent coïncider sans que l'une des conditions a,b,c soit vérifiée. Ils coïncident toujours par exemple lorsque E est un module projectif de rang 2.

Remarque 2.

Tout automorphisme du A-module E compatible avec la forme B_1 et qui laisse e invariant est un automorphisme de l'algèbre E même lorsque 2 n'est pas régulier.

Cas particulier.

A étant supposé intègre, on étudie le groupe d'automorphismes d'une Q-algèbre E solution du problème 1 pour un A-module de rang 2 sur A (ch. III Th.3.3.5) dans le cas où cette solution est associée à une forme bilinéaire symétrique et possède un idempotent non trivial Y.

Soit $M \oplus T$ la décomposition associée à Y (prop. 4.2.5. cor. 2) les automorphismes de l'algèbre E conservent M et T, ils sont de la forme $(\sigma \oplus 1_T) \circ (1_M \oplus \tau)$ où σ est un automorphisme de l'algèbre quadratique M et τ un automorphisme du module de torsion T compatible avec la multiplication.

Puisque A est intègre et Q non dégénérée sur M, σ est l'identité ou l'automorphisme $X \mapsto B(X,e)\, e - X$, (prop. 1.2.9). Puisque T est de carré nul, tout automorphisme du A-module T est compatible avec la multiplication, donc τ décrit le groupe des automorphisme du A-module T.

Le groupe d'automorphismes de l'algèbre E est le produit direct de deux sous groupes dont l'un est d'ordre 2.

§ 3 - *Q-algèbres non nécessairement commutatives.*

Soit E une Q-algèbre sur A d'unité e (déf. 0.1.2). Pour tout élément X de E :

$$X^2 = - Q(X)\, e + B(X,e)\, X \quad (B \text{ est la forme bilinéaire associée à } Q)$$

et pour tout couple (X,X') d'éléments de E :

$$XX' + X'X = - B(X,X')\, e + B(X,e)\, X' + B(X',e)\, X$$

Lorsque le module quadratique (E,Q) vérifie la propriété (1.2.10)'

(1.2.10)' | Il existe une forme bilinéaire symétrique B_1 définie sur E^2 telle que pour tout élément X de E, $Q(X) = B_1(X,X)$

On peut munir E de la structure de Q-algèbre commutative E_+ dont la multiplication est définie pour tout couple (X,X') d'éléments de E par

$$X \circ X' = X' \circ X = - B_1(X,X')\, e + B_1(X,e)\, X' + B_1(X',e)\, X$$

E_+ est une Q-algèbre selon la définition (4.2.1). $B = 2\, B_1$.

Lorsque 2 est inversible dans A, cette algèbre E_+ existe et est uniquement déterminée par la donnée de l'algèbre E ($X \circ X' = \frac{XX' + X'X}{2}$).

Il en est de même par exemple lorsque (E,Q) vérifiant la propriété (1.2.10)', A est intègre et E sans torsion, ou E libre et 2 régulier.

Il existe des Q-algèbres non commutatives E vérifiant cette propriété, par exemple les algèbres de Cayley et les algèbres de quaternions sur un corps de caractéristique $\neq 2$.

1 - Etude des Q-algèbres non nécessairement commutatives qui possèdent des idempotents non triviaux.

Soit E une Q-algèbre d'unité e. On suppose que A ne possède pas d'idempotents non triviaux. D'après la proposition 4.1.5, les idempotents non

triviaux de E sont les solutions Y du système $(Q(Y) = 0$ et $B(Y,e) = 1)$. On suppose que E possède un idempotent non trivial Y et que le module quadratique (E,Q) vérifie la propriété:

(1.2.10)' | Il existe une forme bilinéaire symétrique B_1 définie sur E^2 telle que pour tout élément X de E, $Q(X) = B_1(X,X)$

Alors 2 est inversible dans A, (car $2\,B_1(Y,e) = 1$), et l'algèbre commutative E_+ associée à E est déterminée de façon unique. Y est aussi un idempotent non trivial de E_+ donc, d'après la proposition 4.2.4.,

Proposition 4.3.1.-

On suppose que A ne possède pas d'idempotents non triviaux. Soit E une Q-algèbre d'unité e non nécessairement commutative telle que le module (E,Q) vérifie la propriété (1.2.10)'. Alors.

A tout idempotent non trivial Y de E, on peut associer une décomposition en somme directe de A-modules $E = E'_Y \oplus E''_Y \oplus E'''_Y$ possédant les propriétés suivantes :

1) Soit $M_Y = E'_Y \oplus E''_Y$; M_Y est une sous-algèbre de E (et de l'algèbre commutative associée E_+), de base $(Y, e - Y)$. $E'_Y = AY$ et $E''_Y = A(e - Y)$ les multiplications de E et de E_+ coïncident sur M_Y.

2) Q n'est pas dégénérée sur M_Y. E'_Y et E''_Y sont des sous-modules totalement isotropes de E et E'''_Y est l'orthogonal de M_Y dans (E,Q).

Remarque.

M_Y est associative mais n'est pas nécessairement une sous-algèbre associative maximale de E (cf. cas commutatif).

En effet, il existe des algèbres de quaternions sur un corps de caractéristique $\neq 2$ qui possèdent des idempotents non triviaux. De telles algèbres sont associatives et de dimension 4.

On va étudier plus particulièrement parmi les algèbres E celles qui sont alternatives.

Par définition, une algèbre est alternative lorsque tous les associateurs qui contiennent deux éléments égaux sont nuls. Une algèbre E alternative est en particulier flexible, $((XY)X = X(YX))$ pour tout couple (X,Y) d'éléments de E).

Décomposition de Peirce dans les Q-algèbres alternatives.

Proposition (4.3.1)'.

On suppose que A n'a pas d'idempotents non triviaux.

Soit E une Q-algèbre d'unité e. On suppose que E est alternative et que le module quadratique (E,Q) vérifie la propriété (1.2.10)'. Alors :

A tout idempotent non trivial Y de E, on peut associer une décomposition en somme directe de A-modules $E = E_{11} \oplus E_{00} \oplus E_{10} \oplus E_{01}$ où $E_{ij} = \{X \mid X \in E, YX = i\,X \text{ et } XY = j\,X\}$ $(i,j = 0 \text{ ou } 1)$ possédant les propriétés suivantes :

$E_{11} = AY$, $E_{00} = A(e - Y)$. Les ensembles E_{ij} sont des sous-modules totalement isotropes de (E,Q) et $E_{10} \oplus E_{01}$ est l'orthogonal de $E_{11} \oplus E_{00}$ dans (E,Q).

(Les ensembles E_{ij} dépendent de Y, on a négligé l'indice Y pour simplifier.)

Preuve.

On utilise les propriétés suivantes établies par exemple dans [3] pour les algèbres alternatives E sur un corps de caractéristique $\neq 2$.

Y désignant un idempotent non trivial de E, E possède la décomposition indiquée dans la proposition, tout élément X de E s'écrivant de façon unique $X = X_{11} + X_{00} + X_{10} + X_{01}$ avec $X_{ij} \in E_{ij}$, $X_{11} = Y\,XY$, $X_{00} = X - XY - YX - Y\,XY$,

$X_{10} = YX - Y\,XY$, $X_{01} = XY - Y\,XY$ (puisque E est flexible, on peut poser $Y(XY) = (YX)\,Y = Y\,XY$.

De plus,

(2) $E'_Y = E_{11}$, $E''_Y = E_{00}$, $E'''_Y = E_{10} \oplus E_{01}$

(3) $\forall\, i,j,k$, $(i,j,k = 0$ ou $1)$, $E_{ij}\,E_{jk} \subset E_{ik}$, $E_{ij}\,E_{ij} \subset E_{ji}$

Ces propriétés s'étendent facilement à une algèbre alternative sur un anneau A dans lequel 2 est inversible.

Une Q-algèbre E qui vérifie les hypothèses de la proposition (4.3.1)' et qui possède un idempotent non trivial Y admet donc la décomposition indiquée dans cette proposition. Avant de montrer que les ensembles E_{ij} sont totalement isotropes, on va préciser les propriétés de la multiplication dans E.

Soient X et X' deux éléments de E, on étudie différents cas

– $\underline{X \in E_{10},\ X' \in E_{01}}$

Puisque $E_{10} \oplus E_{01} = (E_{11} \oplus E_{00})^{\perp}$, $B(X,e) = B(X',e) = 0$ et $XX' + X'X = -B(X,X')e$ donc $XX' + X'X = -B(X,X')\,Y - B(X,X')\,(e - Y)$

Compte tenu de (3), $\underline{XX' = -B(X,X')\,Y}$ et $\underline{X'X = -B(X,X')\,(e - Y)}$

– $\underline{X \in E_{10},\ X' \in E_{10}}$

$XX' + X'X = -B(X,X')\,e$, XX' et $X'X \in E_{01}$

Donc $\underline{XX' + X'X = 0}$ et puisque e est libre $\underline{B(X,X') = 0}$

En particulier pour tout élément X de E_{10}, $X^2 = 0$ et $\underline{Q(X) = 0}$

– $\underline{X \in E_{01},\ X' \in E_{01}}$

Les résultats sont analogues aux précédents $XX' \in E_{10}$ et $X'X \in E_{10}$

— $X \in E_{10}$, $X' \in E_{11} \oplus E_{00}$

si $X' = a\,Y + b(e - Y)$, $XX' = b\,X$ et $X'X = a\,X$

— $X \in E_{01}$, $X' \in E_{11} \oplus E_{00}$

si $X' = a\,Y + b(e - Y)$, $XX' = a\,X$ et $X'X = b\,X$

Conséquences.

La multiplication d'un élément de E_{ij} par un élément de $E_{k\ell}$ est déterminée par la donnée de la forme B sauf lorsque $i = k$ et $j = \ell$.

Les ensembles E_{ij} sont totalement isotropes. En effet, on sait déjà que E_{11} et E_{00} sont totalement isotropes et l'étude du deuxième et du troisième cas montre qu'il en est de même pour E_{10} et E_{01} .

Proposition 4.3.2.-

On suppose que A n'a pas d'idempotents non triviaux. Soit E une Q-algèbre qui vérifie les hypothèses de la proposition (4.3.1.)' et qui possède un idempotent non trivial Y. Soient K_1 le noyau du module quadratique (E,Q) et $E_{11} \oplus E_{00} \oplus E_{10} \oplus E_{01}$ la décomposition associée à Y. Les propriétés suivantes sont équivalentes.

1) $E_{10} \oplus E_{01} = K_1$

2) $E_{10} \oplus E_{01}$ est un idéal bilatère de E.

Preuve.

$E_{10} \oplus E_{01} = E'''$ (prop. 4.3.1.). Tout idéal bilatère de E est un idéal de l'algèbre commutative associée E_+ . Donc si E''' est un idéal bilatère de E, $E''' = K_1$ (prop. 4.2.5.).

Inversement, les calculs précédents montrent que lorsque $K_1 = E'''$, E''' est un idéal bilatère de E.

Remarque.

Lorsque $E''' = K_1$, la forme Q est multiplicative sur E. Mais la forme Q peut être multiplicative sur E sans que K_1 soit égal à E'''.

En effet, la norme réduite d'une algèbre de quaternions est multiplicative et non dégénérée donc les algèbres de quaternions, (sur un corps de caractéristique $\neq 2$ par exemple) qui possèdent des idempotents non triviaux fournissent des contre exemples ($E''' \neq (0)$ et $K_1 = (0)$).

L'étude des formes multiplicatives sur E sera faite dans le chapitre V.

Le groupe des transformations orthogonales de (E,Q) qui laissent e invariant est le groupe des automorphismes de l'algèbre E_+ (prop. 4.2.5). Il ne coïncide pas avec le groupe des automorphismes de l'algèbre E lorsque cette algèbre n'est pas commutative. On a par exemple le résultat suivant :

Proposition 4.3.3.-

On suppose que A n'a pas d'idempotents non triviaux. Soit E une Q-algèbre qui vérifie les hypothèses de la proposition (4.3.1.)' et qui possède un idempotent non trivial. L'automorphisme σ du A-module E défini par $\sigma(X) = B(X,e)\, e - X$ est une involution de l'algèbre E.

Preuve.

Soit Y un idempotent non trivial de E et soit $E_{11} \oplus E_{00} \oplus E_{10} \oplus E_{01}$ la décomposition associée à Y. On vérifie facilement à l'aide du tableau précédent que pour tout couple (X,X') d'éléments de E, $\sigma(XX') = \sigma(X')\,\sigma(X)$. (Soient par exemple $X \in E_{10}$ et $X' \in E_{01}$, alors $\sigma(X) = -X$ $\sigma(X') = -X'$, $\sigma(X')\,\sigma(X) = X'X$ et $\sigma(XX') = \sigma(-B(X,X')\,Y) = -B(X,X')\,(e - Y) = X'X$). σ est une transformation orthogonale de E qui laisse e invariant mais lorsque E n'est pas commutative, il existe X et X' tels que $\sigma(XX')$ et $\sigma(X)\,\sigma(X')$ soient distincts.

Conséquence de la proposition 4.3.3. :

Proposition 4.3.4.-

On suppose que A n'a pas d'idempotents non triviaux. Soit E une Q-algèbre d'unité e qui vérifie les hypothèses de la proposition (4.3.1.)' et qui possède un idempotent non trivial. La forme linéaire $X \mapsto B(X,e)$ e est associative sur E. Autrement dit, elle s'annule sur les associateurs et commutateurs de E.

Preuve.

Pour tout couple (X,X') d'éléments de E

$$\sigma(XX') - \sigma(X')\,\sigma(X) = B(XX',e)\,e - XX' - [B(X',e)\,e - X'][B(X,e)\,e - X]$$

$$= B(XX',e)\,e - B(X,e)\,B(X',e)\,e - 2(X\circ X') + B(X,e)\,X' + B(X',e)X$$

$$= [B(X,X')\,e - B(X,e)\,B(X',e) + B(X,X')]\,e$$

car $2\,X \circ X' = XX' + X'X = -B(X,X')\,e + B(X,e)\,X' + B(X',e)\,X$

De cette dernière relation , on déduit également

$$B(X\circ X',e) = -B(X,X') + B(X,e)\,B(X',e)$$

d'où

$$\sigma(XX') - \sigma(X')\,\sigma(X) = [B(XX',e) - B(X\circ X',e)]\,e$$

et puisque $\sigma(XX') = \sigma(X')\,\sigma(X)$ (prop. 4.3.3.).

$$B(XX',e) = B(X\circ X',e) = B(X'X,e)$$

Donc la forme $X \mapsto B(X,e)$ s'annule sur les commutateurs de E.

D'autre part, puisque E est flexible, on a pour tout ensemble (X,X',X") d'éléments de E

$$(X+X")\,[X'(X+X")] = [(X+X")X']\,(X+X")$$

et après réduction

$$X(X'X'') + X''(X'X) = (XX')\,X'' + (X''X')\,X$$

donc

(4) $\quad B(X(X'X''),e) + B(X''(X'X),e) = B((XX')\,X'',e) + B((X''X')\,X,e)$

de plus, puisque la forme $X \to B(X,e)\,e$ est associative sur E_+ (prop. 4.2.3).

$$B(Xo(X'oX''),\ e) = B(X''o(XoX'),\ e)$$

d'où $2\,B(X(X'oX''),\ e) = 2\,B(X''(XoX'),\ e)$ c'est à dire

(5) $\quad B(X(X'X''),e) + B(X(X''X'),\ e) = B(X''(XX'),e) + B(X''(X'X),\ e)$

(4) et (5) impliquent $\quad 2\left[B(X(X'X''),e) - B((XX')X'',e)\right] = 0$

Donc la forme $X \mapsto B(X,e)$ s'annule sur les associateurs de E.

Remarque.

Toute Q-algèbre flexible sur un corps de caractéristique $\neq 2$ possède aussi les propriétés 4.3.3. et 4.3.4. [1] . Il est immédiat que ces propriétés restent vraies lorsque A est intègre, 2 inversible et l'algèbre sans torsion même lorsque l'algèbre n'a pas d'idempotents non triviaux.

CHAPITRE V

FORMES QUADRATIQUES MULTIPLICATIVES SUR UNE Q-ALGEBRE.

---

§ 1 - *Formes quadratiques multiplicatives sur une algèbre quadratique* (algèbre unitaire libre de rang 2).

Pour le moment, on ne fait pas de restriction sur l'anneau A. Soit E une algèbre quadratique sur A de norme Q. Il existe toujours au moins une forme quadratique multiplicative définie sur E, la norme Q (prop. 1.2.1.). De plus :

Proposition 5.1.1.-

Soit E une algèbre quadratique sur A. Toute forme quadratique multiplicative définie sur E, distincte de la norme, est dégénérée.

Preuve.

Soit E une algèbre quadratique d'unité e, de base (e,i) telle que $i^2 = \alpha e + \beta i$, $(\alpha,\beta \in A)$. La norme Q de E est la forme quadratique définie par $Q(e) = 1$, $Q(i) = -\alpha$, $B(e,i) = \beta$.

Par définition, une forme quadratique Q' définie sur E est multiplicative lorsque $Q'(e) = 1$ et lorsque pour tout couple (X_1,X_2) d'éléments de E, $Q'(X_1X_2) = Q'(X_1)Q'(X_2)$.

Si on pose $Q'(i) = -\alpha'$, $B'(e,i) = \beta'$, cette dernière condition s'écrit, compte tenu de $Q'(e) = 1$, pour $X_1 = x_1e + y_1i$ et $X_2 = x_2e + y_2i$:

$$(x_1^2 + \beta' x_1y_1 - \alpha' y_1^2)(x_2^2 + \beta' x_2y_2 - \alpha' y_2^2) =$$

$$= (x_1x_2+\alpha y_1y_2)^2+\beta'(x_1x_2+\alpha y_1y_2)(x_1y_2+x_2y_1+\beta y_1y_2)-\alpha'(x_1y_2+x_2y_1+\beta y_1y_2)^2$$

et après réduction,

$$(2\alpha'-2\alpha+\beta'^2-\beta\beta')x_1x_2y_1y_2 + (-\alpha\beta'-\alpha'\beta'+2\alpha'\beta)(y_1^2x_2y_2+y_2^2x_1y_1)$$

$$+ (\alpha'^2-\alpha^2-\alpha\beta\beta'+\alpha'\beta^2)y_1^2y_2^2 = 0$$

Déterminer les formes quadratiques multiplicatives Q' revient à trouver les couples (α',β') vérifiant cette équation quels que soient les éléments x_1,x_2,y_1,y_2 de A. Ce sont les solutions du système

$$(5.1.1.)\qquad \left|\begin{array}{ll} 2\alpha' - 2\alpha + \beta'^2 - \beta\beta' = 0 & (1)\\ 2\alpha'\beta - \alpha\beta' - \alpha'\beta' = 0 & (2)\\ \alpha'^2 - \alpha^2 - 2\beta\beta' + \alpha'\beta^2 = 0 & (3)\end{array}\right.$$

Les équations (1) et (2) s'écrivent

$$2(\alpha' - \alpha) + \beta'(\beta' - \beta) = 0$$

$$\beta'(\alpha' - \alpha) - 2\alpha'(\beta' - \beta) = 0$$

Pour que ce dernier système admette une solution non nulle en $\alpha' - \alpha$, $\beta' - \beta$, il faut que le déterminant $-(4\alpha'+\beta'^2)$ soit un élément non régulier de A.

Autrement dit, s'il existe une forme quadratique multiplicative sur E distincte de Q, cette forme est dégénérée.

1 - Etude du problème lorsque A est intègre.

Proposition 5.1.2.-

On suppose A intègre. Soit E une algèbre quadratique d'unité e, du base (e,i) telle que $i^2 = \alpha e + \beta i$. Il existe zéro ou deux formes quadratiques multiplicatives sur E distinctes de la norme Q de E. Il n'en existe pas lorsque Q est dégénérée.

Lorsque de plus la propriété (1.2.10) est vérifiée, ($2 \neq 0$ et $\beta \in 2A$), pour qu'il existe deux formes quadratiques multiplicatives sur E distinctes de Q, il faut et il suffit que $4\alpha+\beta^2$ soit le carré d'un élément de A.

Preuve.

Lorsque $2 = 0$, le système (5.1.1.) devient

$\beta'(\beta - \beta') = 0$

$\beta'(\alpha - \alpha') = 0$

$$\alpha'^2 - \alpha^2 - \alpha\beta\beta' + \alpha'\beta^2 = 0$$

Pour toute solution (α',β') distincte de (α,β) , $\beta' = 0$ et $\alpha'^2 - \alpha^2 + \alpha'\beta^2 = 0$.

Lorsque $\beta = 0$, c'est-à-dire lorsque Q est dégénérée, la seule solution est (α,β).

Lorsque $\beta \neq 0$, les solutions distinctes de la solution (α,β) sont les couples $(\alpha',0)$ tels que $\alpha'^2 - \alpha^2 + \alpha'\beta^2 = 0$. Il existe donc au plus deux formes Q' distinctes de Q. Lorsqu'il en existe une, il en existe deux car la somme β^2 des racines de la dernière équation n'est pas nulle.

Lorsque $2 \neq 0$, il est facile de voir que le système (5.1.1.) est équivalent au système

$$2(\alpha' - \alpha) + \beta'(\beta' - \beta) = 0$$
$$(4\alpha' + \beta'^2)(\beta' - \beta) = 0$$
$$(\alpha - \alpha')[2(\alpha + \alpha') + \beta\beta'] = 0$$

Un couple (α',β') est une solution si et seulement si il vérifie (5.1.1.)' ou (5.1.1.)" avec

$$(5.1.1.)' \begin{cases} 2(\alpha' - \alpha) + \beta'(\beta' - \beta) = 0 \\ (4\alpha' + \beta'^2)(\beta' - \beta) = 0 \\ \alpha - \alpha' = 0 \end{cases} \qquad (5.1.1.)'' \begin{cases} 2(\alpha' - \alpha) + \beta'(\beta' - \beta) = 0 \\ (4\alpha' + \beta'^2)(\beta' - \beta) = 0 \\ 2(\alpha + \alpha') + \beta\beta' = 0 \end{cases}$$

Lorsque le système (5.1.1.)' admet une solution (α',β') distincte de (α,β), $\alpha' = \beta' = 0$. Ce cas ne peut se présenter que lorsque $\alpha = 0$ et $\beta \neq 0$. Q est alors non dégénérée.

Les solutions du système (5.1.1.)" distinctes de la solution éventuelle (α,β) sont les solutions distinctes de (α,β) du système

$$(4) \qquad \beta'^2 - 2\beta\beta' - 4\alpha = 0$$
$$(5) \qquad 4\alpha' + \beta'^2 = 0$$

Pour que ce dernier système admette une solution, il faut que $4\alpha+\beta^2$ soit le carré d'un élément de A.

Lorsque $4\alpha+\beta^2 = 0$, la seule solution est (α,β).

Lorsque $4\alpha+\beta^2 \neq 0$ et lorsqu'il existe des solutions, il en existe deux et elles sont distinctes de (α,β).

On voit en particulier que lorsque β est multiple de 2 le système (5.1.1.)" admet deux solutions distinctes de (α,β) exactement lorsque $4\alpha+\beta^2$ est le carré d'un élément non nul de A.

Lorsque $\alpha = 0$, $\beta \neq 0$, le système (5.1.1.)" redonne la solution $(0,0)$ du système (5.1.1.)'.

Corollaire 1.

On suppose A intègre. Soit E une algèbre quadratique d'unité e et de norme Q. Lorsqu'il existe une forme quadratique Q' multiplicative sur E, la forme Q n'est pas multiplicative sur l'algèbre quadratique de module sous-jacent E, d'unité e, de norme Q'.

En effet, d'après la proposition 5.1.1., Q' est dégénérée. Donc, d'après la proposition 5.1.2., Q' est la seule forme quadratique multiplicative sur l'algèbre de module sous-jacent E, d'unité e et de norme Q'.

Corollaire 2.

On suppose que A est intégralement clos. Soit E une algèbre quadratique d'unité e, de norme Q telle que le module quadratique (E,Q) vérifie la propriété (1.2.10). Alors, pour qu'il existe deux formes quadratiques multiplicatives sur E distinctes de Q, il faut et il suffit que $K_1 = (0)$ et $H \neq (0)$ (K_1 est le noyau du module quadratique (E,Q) et H l'ensemble des éléments isotropes).

La condition est nécessaire. En effet :

Soit (e,i) une base de E telle que $i^2 = \alpha e + \beta i$. Lorsqu'il existe deux formes quadratiques multiplicatives sur E distinctes de Q, $4\alpha + \beta^2$ est le carré d'un élément non nul de A, (prop. 5.1.2.). Donc $K_1 = (0)$ et l'équation $(x + \frac{\beta}{2} y)^2 - (\frac{4\alpha+\beta^2}{4})y^2 = 0$, $(Q(xe + yi) = 0)$, admet des solutions non nulles.

Elle est suffisante. En effet :

Lorsque H n'est pas nul, $\frac{4\alpha+\beta^2}{4}$ est un carré dans le corps des fractions de A donc est le carré d'un élément de A. Lorsque de plus $K_1 = (0)$, ce carré n'est pas nul. Donc, (prop. 5.1.2.), il existe deux formes quadratiques multiplicatives sur E distinctes de Q.

Corollaire 3.

On suppose que A est un corps de caractéristique $\neq 2$. Soit E une algèbre quadratique sur A d'unité e, de norme Q. Alors, pour qu'il existe sur E deux formes quadratiques multiplicatives distinctes de Q, il faut et il suffit que l'une des conditions équivalentes suivantes soit vérifiée

1.- $K_1 = (0)$ et $H \neq (0)$

2.- E possède des idempotents non triviaux.

Preuve.

2 est inversible et A intégralement clos donc la condition (1) est nécessaire et suffisante (cor. 2).

1 <==> 2 en effet

Lorsque $K_1 = (0)$ et $H \neq (0)$, il existe au moins un élément X de E tel que $Q(X) = 0$ et $B(X,e) \neq 0$. Alors l'élément $\frac{X}{B(X,e)}$ est un idempotent non trivial de E (prop. 4.1.5.). Inversement, lorsque E possède un idempotent non trivial, H n'est pas nul et Q n'est pas dégénérée(prop. 4.2.4.).

2 - Propriétés des formes quadratiques multiplicatives sur E et des algèbres associées.

Proposition 5.1.3.-

On suppose A intègre. Soit E une algèbre quadratique sur A d'unité e de norme Q. Lorsqu'il existe deux formes quadratiques Q' et Q" multiplicatives sur E et distinctes de Q, on a, pour tout élément X de E, $(Q(X))^2 = Q'(X)Q''(X)$.

Preuve.

Soit (e,i) une base de E telle que $i^2 = \alpha e + \beta i$. Les formes Q' et Q'' sont associées aux deux solutions (α',β') et (α'',β'') distinctes de (α,β) du système (5.1.1.). On utilise les calculs de la preuve de la proposition 5.1.2.

Lorsque $2 = 0$ $\beta' = \beta'' = 0$, α' et α'' sont les racines de l'équation $t^2 + t\beta^2 + \alpha^2 = 0$. Soit X un élément de E, $(X = xe + yi)$.

$$Q'(X)Q''(X) = (x^2 - \alpha' y^2)(x^2 - \alpha'' y^2) = (x^2 + \beta xy - \alpha y^2)^2 = (Q(X))^2,$$

compte tenu de $\alpha' + \alpha'' = \beta^2$ et $\alpha'\alpha'' = \alpha^2$.

Lorsque $2 \neq 0$; $4\alpha' + \beta'^2 = 4\alpha'' + \beta''^2 = 0$, β' et β'' sont les racines de l'équation $t^2 - 2\beta t - 4\alpha = 0$.

$$4Q'(X) = (2x + \beta' y)^2 \quad , \quad 4Q''(X) = (2x + \beta'' y)^2$$

$$16Q'(X)Q''(X) = (2x+\beta' y)^2(2x+\beta'' y)^2 = 16(x^2+\beta xy-\alpha y^2)^2 = 16(Q(X))^2$$

compte tenu de $\beta' + \beta'' = 2\beta$ et $\beta'\beta'' = -4\alpha$. Donc $Q'(X)Q''(X) = Q^2(X)$.

Soit E', (resp. E''), l'algèbre quadratique d'unité e, de norme Q', (resp. Q'') de module sous jacent E. De même qu'on a associé à (E,Q) les ensembles H,K,K_1, (déf. 0.1.1.), on associe à (E,Q'), (resp. E,Q''), les ensembles H',K',K_1', (resp. H'', K'', K_1'').

On sait que Q' et Q'' sont dégénérées, c'est-à-dire que $K' \neq (0)$ et $K'' \neq (0)$. D'autre part, puisque A est intègre et $K' \neq (0)$, $H' = K_1'$ et H' est un idéal premier de E', nilradical de E' (prop. 1.2.5.). De même, $H'' = K_1''$ et K_1'' est le nilradical de E''.

Proposition 5.1.4.-

On suppose A intègre. Soit E une algèbre quadratique sur A d'unité e, de norme Q. On suppose qu'il existe deux formes quadratiques Q' et Q'' multiplicatives sur E et distinctes de Q. On désigne par E', (resp. E'') l'algèbre quadratique d'unité e, de norme Q', (resp. Q''), de module sous-jacent E. Alors :

Les éléments réguliers de E sont les éléments réguliers dans E' ou dans E". Avec les notations (0.1.1.), H' et H" sont des idéaux premiers de E, $H = H' \cup H''$, $H' \cap H'' = (0)$.

Preuve.

Les éléments réguliers d'une algèbre quadratique sont les éléments de norme régulière. La première partie de la proposition est donc une conséquence de la proposition précédente ainsi que l'égalité $H = H' \bigcup H''$.

Pour tout élément X' de H' et tout élément X de E, $Q'(XX') = Q'(X)Q'(X') = 0$, donc XX' appartient à H'. Comme H' est un sous-module de E, H' est un idéal de E.

H' est premier. En effet $Q'(XX') = 0$ implique $Q'(X) = 0$ ou $Q'(X') = 0$. De même H" est un idéal premier de E.

Compte tenu des relations qui lient α, α', β'', β, β', β'' (notations précédentes)

$(Q'(X) = 0$ et $Q''(X) = 0)$ implique $X = 0$. Donc $H' \cap H'' = (0)$.

Remarque 1.

Les idéaux de rang 1 de E sont les idéaux non nuls de E contenus dans H' ou dans H", H' et H" sont les idéaux I_1 et I_2 de l'étude p. 17 .

Remarque 2.

Lorsque 2 est inversible dans A et lorsque E possède un idempotent non trivial, E est isomorphe à $A \times A$. Les résultats précèdents deviennent alors triviaux. Il en est ainsi par exemple lorsque A est un corps de caractéristique $\neq 2$ et lorsque Q' et Q" existent (prop. 5.1.2. cor. 3) on peut se ramener à ce cas particulier par une extension des scalaires dans le cas où A est intègre et $2 \neq 0$ pour obtenir plus rapidement les résultats précédents.

Automorphismes des algèbres E, E', E".

Lorsqu'il existe deux formes multiplicatives sur E distinctes de la norme Q, Q n'est pas dégénérée donc E possède exactement deux automorphismes,

l'identité et l'automorphisme $\sigma : X \to B(X,e)e - X$.

Proposition 5.1.5.-

Les hypothèses et notations sont celles de la proposition 5.1.4. Soit σ l'automorphisme $X \to B(X,E)e - X$ de E. On désigne par T' et T" les groupes d'automorphismes des algèbres E' et E". Alors, σ est un isomorphisme d'algèbres de E' sur E", $T' = \sigma T" \sigma$ et $T" = \sigma T' \sigma$.

Preuve.

σ est un automorphisme du A-module sous-jacent à E' et E" tel que $\sigma(e) = e$. Soit ϕ', (resp. $\phi"$), l'application bilinéaire qui définit la multiplication de E', (resp.. E"), et soit (e,i) une base de E.

$\sigma(\phi'(i,i)) = (\alpha' + \beta\beta')e - \beta' i$, $\phi"(\sigma(i),\sigma(i)) = (\beta^{2} + \alpha")e + (-2\beta + \beta")i$

(notations des preuves précédentes).

L'égalité de $\sigma(\phi'(i,i))$ et de $\phi"(\sigma(i),\sigma(i))$ résulte des relations entre $\alpha, \alpha', \alpha", \beta, \beta', \beta"$. Le reste de la preuve est immédiat. T' et T" sont des sous groupes conjugués dans le groupe des automorphismes du A-module E. ($\sigma = \sigma^{-1}$).

Extension de l'étude précédente aux algèbres projectives de rang 2.

On suppose toujours A intègre. Soit E une algèbre unitaire projective de rang 2 sur A. E se plonge dans l'algèbre quadratique E_0 obtenue par extension des scalaires au corps des fractions A_0 de A. Alors, il existe sur E zéro ou deux formes quadratiques multiplicatives Q' et Q" distinctes de la norme Q. (On le voit en localisant et globalisant). Lorsqu'elles existent, les formes Q' et Q" sont dégénérées, Q n'est pas dégénérée et les algèbres E' et E" associées à Q' et Q" vérifient les propriétés énoncées dans les propositions 5.1.4. et 5.1.5.

De plus, lorsque A est intégralement clos et lorsque (E,Q) vérifie la propriété (1.2.10), les formes Q' et Q" existent si et seulement si $H \neq \{0\}$

et $K = (0)$. On utilise une méthode de localisation et globalisation et le corollaire 2 de la proposition 5.1.2. pour les algèbres quadratiques E_p, ($p \in \mathrm{Spec}\ A$).

Le paragraphe suivant donnera en particulier quelques résultats complémentaires pour les algèbres de rang 2 qui possèdent des idempotents non triviaux.

§ 2 - *Formes quadratiques multiplicatives sur les Q-algèbres commutatives associées à une forme bilinéaire symétrique.*

Une Q-algèbre associée à une forme bilinéaire symétrique est une Q-algèbre selon la définition 4.2.1.

(Lorsque E est une Q-algèbre d'unité e associée à la forme bilinéaire B_1, on a pour tout élément X de E, $Q(X) = B_1(X,X)$ et pour tout couple (X,X') d'éléments de E, $XX' = -B_1(X,X')e + B_1(X,e)X' + B_1(X',e)X$ et $B(X,X') = 2B_1(X,X')$).

1 - Cas des algèbres qui possèdent des idempotents non triviaux.

Proposition 5.2.1.-

On suppose que A ne possède pas d'idempotents non triviaux. Soit E une Q-algèbre d'unité e associée à la forme bilinéaire symétrique B_1 qui possède un idempotent non trivial Y et soit $E' \oplus E'' \oplus E'''$ la décomposition de Peirce associée à Y.

Alors il existe exactement zéro ou trois formes quadratiques multiplicatives sur E.

Pour que les trois formes existent, il faut et il suffit que l'une des conditions équivalentes ci-dessous soit vérifiée

(I) Q est multiplicative sur E

(II) E''' est un idéal de E

(III) $E''' = K_1$ (K_1 noyau du module quadratique (E,Q)).

Preuve.

L'équivalence des trois conditions résulte de la proposition 4.2.5. Les hypothèses impliquent que 2 est inversible dans A ($2B_1(Y,e) = 1$).

Pour qu'une forme quadratique Q' définie sur E soit multiplicative, il faut que :

(6) $[Q'(Y)]^2 = Q'(Y^2) = Q'(Y)$

(7) $[Q'(e-Y)]^2 = Q'((e-Y)^2) = Q'(e-Y)$

(8) $0 = Q'[Y(e-Y)] = Q'(Y)Q'(e-Y)$.

Puisque 1 et 0 sont les seuls idempotents de A, (6) et (7) impliquent $(Q'Y) = 0$ ou $Q'(Y) = 1)$ et $(Q'(e-Y) = 0$ ou $Q'(e-Y) = 1)$.

Il y a quatre cas à examiner

a) $Q'(Y) = 0$ et $Q'(e-Y) = 0$

b) $Q'(Y) = 0$ et $Q'(e-Y) = 1$

c) $Q'(Y) = 1$ et $Q'(e-Y) = 0$

d) $Q'(Y) = 1$ et $Q'(e-Y) = 1$

Le cas (d) est à exclure car il est incompatible avec la condition (8).

- Toute forme Q' multiplicative sur E est nulle sur E'''. En effet :

$\forall X''' \in E'''$, $X''' = 2 X''' Y = 2 X''' (e-Y)$

$$Q'(X''') = 4 Q'(Y)Q'(X''') = 4 Q'(e-Y)Q'(X''')$$

puisque Q' vérifie les conditions a, b, ou c, $Q'(X''') = 0$.

- Soit B' la forme bilinéaire associée à Q'

$\forall X''' \in E'''$, $B'(Y,X''') = 2 B'(Y^2,YX''') = 2 Q'(Y)B'(Y,X''')$

$$B'(e-Y,X''') = 2 B'((e-Y)^2,(e-Y)X''') = 2 Q'(e-Y)B'(e-Y,X''')$$

ce qui implique $B'(Y,X''') = B'(e-Y,X''') = 0$ dans le cas (a), $B'(Y,X''') = 0$ dans le cas (b) et $B'(e-Y,X''') = 0$ dans le cas (c).

D'autre part, dans le cas (b), puisque $Q'(e-Y) = 1$

$B'(2-Y,X''') = Q'(e-Y)B'(e-Y)X''') = B'((e-Y)^2,(e-Y)X''') = \frac{1}{2} B'(e-Y,X''')$ donc $B'(e-Y,X''') = 0$.

De même dans le cas (c) puisque $Q'Y) = 1$

$B'(Y,X''') = Q'(Y)B'(Y,X''') = B'(Y^2,YX''') = \frac{1}{2} B'(Y,X''')$ donc $B'(Y,X''') = 0$.

En définitive, le noyau de toute forme quadratique multiplicative sur E contient E'''.

Il existe exactement trois formes quadratiques Q' définies sur E dont le noyau contient E''', telles que (a), (b) ou (c) soit vérifié et telles que $Q'(e) = 1$. Elles admettent pour noyaux respectifs E''', $AY \oplus E'''$, $A(e-Y) \oplus E'''$. Il existe donc au plus trois formes quadratiques multiplicatives sur E.

Il reste à examiner si les trois formes peuvent effectivement être multiplicatives.

Soit Q' l'une des trois formes. Pour que Q' soit multiplicative il faut que pour tout couple (Z_1,Z_2) d'éléments de E'''

$$Q'(Z_1Z_2) = Q'(Z_1)Q'(Z_2) \quad \text{et} \quad Q'[(e + Z_1)(e + Z_2)] = Q'(e + Z_1)Q'(e + Z_2) .$$

$Z_1Z_2 = -\dfrac{B(Z_1,Z_2)}{2} e$, $Q'(Z_1) = Q'(Z_2) = 0$ donc il faut que

$$0 = Q'(Z_1)Q'(Z_2) = Q'(Z_1Z_2) = \frac{B^2(Z_1,Z_2)}{4} .$$

$Q'(e + Z_1) = Q'(e + Z_2) = 1$ donc il faut que

$$1 = Q'(e + Z_1)Q'(e + Z_2) = Q'\left(e + Z_1 + Z_2 - \frac{B(Z_1,Z_2)}{2} e\right) = 1 + \frac{B^2(Z_1,Z_2)}{4} - B(Z_1,Z_2) .$$

Donc pour que l'une au moins des trois formes soit multiplicative il faut que pour tout couple (Z_1,Z_2) d'éléments de E''', $B(Z_1,Z_2) = 0$, c'est-à-dire, puisque E''' est orthogonal à $E' \oplus E''$ pour Q, que $K_1 = E'''$.

Il est immédiat que lorsque cette condition est vérifiée les trois formes sont multiplicatives et que la première (cas a) est la forme 2.

Corollaire.

Lorsque A n'a pas d'idempotents non triviaux et lorsque 2 est inversible dans A, il existe trois formes quadratiques multiplicatives sur toute algèbre quadratique sur A qui possède un idempotent non trivial (Une telle algèbre est d'ailleurs isomorphe à $A \times A$).

Remarque.

Lorsque A peut posséder des idempotents non triviaux et lorsque E possède un idempotent Y tel que $Q(Y) = 0$ et $B(Y,e) = 1$ (ce qui implique que 2 est inversible), on a l'extension ci-dessous de la proposition 5.2.1 .

Proposition 5.2.1'.-

Soit E une Q-algèbre d'unité e associée à une forme bilinéaire symétrique B_1 qui possède un idempotent Y tel que $Q(Y) = 0$ et $2\,B_1(Y,e) = 1$

Pour qu'il existe une forme quadratique multiplicative sur E, il faut et il suffit que Q soit multiplicative. Lorsque cette condition est vérifiée, il existe au moins trois formes quadratiques multiplicatives sur E.

Preuve.

Soit Q' une forme quadratique définie sur E telle que $Q'(e) = 1$. E admet la décomposition $AY \oplus A(e-Y) \oplus E'''$ (remarque 2 prop. 4.2.4.). On pose $Q'(Y) = a$ $B'(e,Y) = b$. Pour que Q' soit multiplicative sur E il faut que $Q'(Y)$ et $Q'(e-Y)$ soient des idempotents de A et que $Q'(Y)Q'(e-Y) = 0$ donc que a et $1+a-b$ soient des idempotents et que $2a = ab$.

Par des calculs analogues aux précédents on montre facilement que le noyau de toute forme Q' multiplicative sur E contient E''' (Exemple de calcul : $\forall\, Z \in E'''$, $B'(Y,Z) = B'(Y^2, 2\,YZ) = 2a\,B'(Y,Z)$ où $a = Q'(Y)$ puisque a est un idempotent de A, $2a\,B'(Y,Z) = 2\,a^2\,B'(Y,Z) = a\,B'(Y,Z)$ donc $a\,B'(Y,Z) = 0$ et par suite $B'(Y,Z) = 0$).

On en déduit comme dans la preuve précédente que lorsqu'il existe une forme quadratique multiplicative sur E, $K_1 = E'''$ ou ce qui est équivalent que Q est multiplicative sur E ou encore que E''' est un idéal de E. On suppose cette condition vérifiée.

Puisque le noyau de toute forme quadratique multiplicative contient l'idéal E''', les formes cherchées correspondent uniquement aux formes quadratiques

multiplicatives sur l'algèbre quadratique $AY \oplus A(e-Y)$. Il est immédiat qu'il existe au moins trois formes quadratiques multiplicatives sur $AY \oplus A(e-Y)$ mais lorsque A possède des idempotents non triviaux, il en existe plus comme le montre l'étude du système 5.1.1. du § 1 avec $\alpha = 0$ et $\beta = 1$. (En plus des solutions $(0,1)$, $(0,0)$ et $(-1,2)$ de ce système on trouve par exemple les solutions $(0,\beta')$ où β' est un idempotent non trivial de A).

Etude des algèbres associées aux formes multiplicatives sur E.

Les propriétés suivantes sont immédiates.

On suppose que A ne possède pas d'idempotents non triviaux. Soit E une Q-algèbre d'unité e associée à une forme bilinéaire B_1 qui possède un idempotent non trivial Y et soit $E' \oplus E'' \oplus E'''$ la décomposition associée à Y. On suppose que Q est multiplicative sur E, $(K_1 = E''')$, et on désigne par $Q^{(2)}$ et $Q^{(3)}$ les deux autres formes quadratiques multiplicatives sur E, par $E^{(2)}$, (resp. $E^{(3)}$), la $Q^{(2)}$-algèbre, (resp. $Q^{(3)}$-algèbre) d'unité e, de module sous-jacent E, par $T^{(2)}$, (resp. $T^{(3)}$), le groupe d'automorphismes de $E^{(2)}$, (resp. $E^{(3)}$).

Alors, pour tout élément X de E, $[Q(X)]^2 = Q^{(2)}(X)Q^{(3)}(X)$.

- Les algèbres $E^{(2)}$ et $E^{(3)}$ sont associatives. L'automorphisme $\sigma : X \to B(X,e)e - X$ du A-module E est un isomorphisme d'algèbres de $E^{(2)}$ sur $E^{(3)}$, (et de $E^{(3)}$ sur $E^{(2)}$), $T^{(2)} = \sigma T^{(3)} \sigma$, $T^{(3)} = \sigma T^{(2)} \sigma$.

On suppose que $Q^{(2)}$ est la forme de noyau $AY \oplus K_1$.

- Lorsque A est réduit, $AY \oplus K_1$, (resp. $A(e-Y) \oplus K_1$) est le nil-radical de $E^{(2)}$, (resp. $E^{(3)}$). Avec les notations habituelles (0.1.1.) $K_1^{(2)} = H^{(2)} = AY \oplus K_1$, $K_1^{(3)} = H^{(3)} = A(e-Y) \oplus K_1$ et K_1 est l'ensemble des éléments nilpotents de E.

En effet, pour tout élément $X = aY + b(e-Y) + X'''$ de E, $(a,b \in A$, $X''' \in E''')$ $Q(X) = ab$, $Q^{(2)}(X) = b^2$, $Q^{(3)}(X) = a^2$ donc $[Q(X)]^2 = Q^{(2)}(X)Q^{(3)}(X)$. $E^{(2)}$, (resp. $E^{(3)}$) est la somme directe de Ae et du noyau $K_1^{(2)}$, (resp. $K_1^{(3)}$) qui est un idéal de carré nul. Les propriétés des algèbres $E^{(2)}$ et $E^{(3)}$ sont

donc immédiates.

L'automorphisme σ conserve Ae et échange les noyaux, d'où le résultat annoncé.

Lorsque A est réduit, l'ensemble des éléments nilpotents de E est l'ensemble des éléments X tels que $Q(X) = B(X,e) = 0$ (prop. 4.1.4. cor. 2). Puisque $B(X,e) = a+b$ et $Q(X) = ab$, X est nilpotent si et seulement si $a = b = 0$.

2 - Formes quadratiques multiplicatives sur une Q-algèbre commutative lorsque A est intègre et $2 \neq 0$.

Soit E une Q-algèbre commutative sur A. On vient de déterminer les formes quadratiques multiplicatives sur E lorsque 2 est inversible et lorsque E possède un idempotent non trivial. On va se ramener à ce cas en utilisant l'algèbre E_0 obtenue par extension des scalaires au corps des fractions A_0 de A.

a) On étudie le cas particulier où A est un corps de caractéristique $\neq 2$.

Lorsque le rang de E est égal à 1, il existe sur E une seule forme quadratique multiplicative. On supposera dans la suite que le rang de E est strictement supérieur à 1.

Le cas où le rang de E est égal à 2 a été étudié dans le paragraphe 1 de ce chapitre (prop. 5.1.2. cor. 3).

Proposition 5.2.2.-

On suppose que A est un corps de caractéristique $\neq 2$. Soit E une Q-algèbre commutative sur A de dimension $\geqslant 2$. Il existe exactement zéro, une ou trois formes quadratiques multiplicatives sur E. Dans les deux derniers cas Q est multiplicative sur E.

Pour que Q soit multiplicative sur E, il faut et il suffit que le noyau K_1 du module quadratique (E,Q) soit de codimension 1 ou 2.

Pour qu'il existe trois formes quadratiques multiplicatives sur E, il

faut et il suffit que H soit distinct de K_1 et K_1 de codimension 2. (H ensemble des éléments isotropes).

Preuve.

Il est connu que les seules algèbres commutatives unitaires sur le corps A sur lesquelles il existe une forme quadratique multiplicative non dégénérée sont les algèbres de dimension 1 ou 2, (voir par ex. [4]).

- Soit E une Q-algèbre commutative d'unité e sur le corps A et soit K_1 le noyau de (E,Q). K_1 est un sous-espace vectoriel de E et e n'appartient pas à K_1, il existe donc une décomposition $E = M \oplus K_1$ où e appartient à M. M est une sous-algèbre de E, (en effet, pour tout couple (X,X') d'éléments de M, $XX' = \frac{1}{2}\left[-B(X,X')e + B(X,e)X' + B(X',e)X\right]$) et il est immédiat que 0 n'est pas dégénérée sur M.

Lorsque Q est multiplicative sur E, elle est multiplicative sur M donc M est de dimension 1 ou 2. Inversement, lorsque M est de dimension 1 ou 2, il est immédiat que Q est multiplicative sur E.

- Lorsqu'il existe sur E une forme quadratique multiplicative Q' distincte de Q, il existe au moins une sous-algèbre de dimension 2 sur laquelle Q et Q' sont multiplicatives et distinctes. Donc, (prop. 5.1.2. cor. 3), E possède au moins un idempotent non trivial Y et dans la décomposition de Peirce associée à Y, $K_1 = E_Y'''$ (prop. 5.2.1.). Donc K_1 est de codimension 2 et puisque $Q(Y) = 0$ et $Y \notin K_1$, $H \neq K_1$.

Inversement lorsque K_1 est de codimension 2 et $H \neq K_1$, E admet une décomposition de la forme $Ae \oplus Ai \oplus K_1$ où $B(e,i) \neq 0$, $Q(i) = 0$. $Y = \frac{i}{B(e,i)}$ est un idempotent non trivial de E et dans la décomposition de Peirce associée à Y, $K_1 = E_Y'''$ (En effet $K_1 \subset E_Y'''$ et E_Y''' est de codimension 2). Il existe alors trois formes multiplicatives sur E (prop. 5.2.1.)

b) <u>On suppose</u> A <u>intègre et</u> $2 \neq 0$.

Proposition 5.2.3.-

On suppose A intègre et $2 \neq 0$. Soit E une Q-algèbre commutative sur A. On désigne par E_0 l'algèbre obtenue par extension des scalaires au corps des fractions A_0 de A, par Q_0 l'extension de Q à E_0, par $K_{1,0}$ le noyau de (E_0, Q_0).

1.- Il existe au plus trois formes quadratiques multiplicatives sur E. Pour qu'il existe plus d'une forme quadratique multiplicative sur E, il faut que K_1 soit distinct de H et $K_{1,0}$ de codimension 2 dans E_0.

2.- Pour que Q soit multiplicative, il faut et il suffit que $K_{1,0}$ soit de codimension 1 ou 2.

Lorsque E est de rang fini n, la condition $K_{1,0}$ est de codimension 1 ou 2 s'écrit K_1 est de rang $n-1$ ou $n-2$.

Preuve.

Une forme quadratique Q' définie sur E est multiplicative sur E si et seulement si son extension Q'_0 à E_0 est multiplicative sur E_0. Il existe donc au plus trois formes quadratiques multiplicatives sur E.

- Lorsqu'il existe au moins deux formes quadratiques multiplicatives sur E, les extensions de ces formes sont distinctes et multiplicatives sur E_0 donc, avec les notations usuelles $K_{1,0}$ est de codimension 2 et distinct de H_0 ce qui implique que H est distinct de K_1.

- Pour que Q soit multiplicative sur E, il faut et il suffit que Q_0 soit multiplicative sur E_0 donc que H_0 soit distinct de $K_{1,0}$ (c'est-à-dire H distinct de K_1) et que $K_{1,0}$ soit de codimension 1 ou 2.

On peut préciser lorsque 2 est inversible dans A.

Proposition 5.2.4.-

On suppose que A est intègre et 2 inversible dans A. Soit E une Q-algèbre commutative sur A d'unité e. Il existe exactement zéro, une ou trois

formes quadratiques multiplicatives sur E.

Lorsque les trois formes Q, $Q^{(2)}$ et $Q^{(3)}$ existent, E admet les décompositions $E = Ae \oplus K_1^{(2)}$ et $E = Ae \oplus K_1^{(3)} = H$ et $K_1^{(2)}$ $K_1^{(3)}$ sont les noyaux de $(E,Q^{(2)})$ et $(E,Q^{(3)})$. $K_1^{(2)} \cup K_1^{(3)} = H$ et $K_1^{(2)} \cap K_1^{(3)} = K_1$.

La $Q^{(2)}$-algèbre, (resp. $Q^{(3)}$-algèbre) commutative $E^{(2)}$, (resp. $E^{(3)}$) d'unité e et de module sous-jacent E est associative, de nilradical $K_1^{(2)}$, (resp. $K_1^{(3)}$). K_1 est l'ensemble des éléments nilpotents de E.

Preuve.

Pour qu'il existe au moins deux formes quadratiques multiplicatives sur E, il faut que $K_{1,0}$ soit de codimension 2 et distinct de H_0. On suppose cette condition vérifiée. E_0 possède alors un idempotent Y_0. Soit f_0 l'homomorphisme canonique de E dans E_0 et soit $E_0 = A_0 Y_0 \oplus A_0(e_0-Y_0) \oplus K_{1,0}$ la décomposition de E_0 associée à Y_0 (on a posé $e_0 = f_0(e)$). Tout élément $f_0(X)$ de $f_0(E)$ s'écrit de façon unique sous la forme

$$f_0(X) = a\,Y_0 + b(e_0 - Y_0) + Z_0 \qquad (a,b \in A_0,\ Z_0 \in K_{1,0}) \tag{9}$$

S'il existe une forme quadratique Q_2 multiplicative sur E, distincte de Q, le noyau $K_{1,0}^{(2)}$ de l'extension $Q_0^{(2)}$ de $Q^{(2)}$ à E_0 est soit $A_0 Y_0 \oplus K_{1,0}$, soit $A_0(e_0 - Y_0) \oplus K_{1,0}$ (étude p. 125). Soit par exemple $K_{1,0}^{(2)} = A_0 Y_0 \oplus K_{1,0}$. Alors, avec les notations habituelles

$$B(X,e) = B_0(f_0(X),e_0) = a+b \ , \ B^{(2)}(X,e) = B_0^{(2)}(f_0(X),e_0) = 2b \ , \ Q^{(2)}(X) = b^2$$

Puisque 2 est inversible et puisque a+b et 2b appartiennent à A, a et b appartiennent à A.

On vérifie facilement que l'application $Q^{(3)}$ de E dans A définie par $Q^{(3)}(X) = a^2$, (où a est défini par l'équation 9) est une forme quadratique multiplicative sur E. Le raisonnement est analogue lorsqu'on remplace $A_0 Y_0 \oplus K_{1,0}$ par $A_0(e_0 - Y_0) \oplus K_{1,0}$.

Donc lorsqu'il existe sur E deux formes quadratiques multiplicatives, il en existe trois, Q, $Q^{(2)}$ et $Q^{(3)}$.

De plus, $f_0(X - be)$ appartient à $K_{1,0}^{(2)}$ donc $X - be$ appartient à $K_1^{(2)}$. Comme $Ae \cap K_1^{(2)} = (0)$, $E = Ae \oplus K_1^{(2)}$. De même $E = Ae \oplus K_1^{(3)}$.

Les propriétés des algèbres E, $E^{(2)}$, $E^{(3)}$ s'établissent comme dans le cas où il existe un idempotent non trivial.

§ 3 - *Formes quadratiques multiplicatives sur les Q-algèbres alternatives.*

Soit E une Q-algèbre sur A. Lorsque 2 est inversible dans A l'algèbre commutative E_+ associée à E est déterminée de façon unique (§ 3. Chap. IV), mais la recherche des formes quadratiques multiplicatives sur E ne se ramène pas à la recherche des formes quadratiques multiplicatives sur E_+. Il peut exister une forme multiplicative sur E qui n'est pas multiplicative sur E_+.

Exemple. E désigne une algèbre de quaternions sur un corps de caractéristique $\neq 2$. La norme réduite Q n'est pas dégénérée, elle est multiplicative sur E mais elle n'est pas multiplicative sur E_+ car E_+ est commutative de dimension $\neq 1$ et $\neq 2$.

1 - Formes quadratiques multiplicatives sur une Q-algèbre alternative qui possède un idempotent non trivial.

Proposition 5.3.1.-

On suppose que A ne possède pas d'idempotents non triviaux et que 2 est inversible dans A. Soit E une Q-algèbre alternative qui possède un idempotent non trivial Y et soit $E_{11} \oplus E_{00} \oplus E_{10} \oplus E_{01}$ la décomposition de Peirce associée à Y.

Il existe zéro, une ou trois formes quadratiques multiplicatives sur E. Pour qu'il existe trois formes multiplicatives sur E, il faut et il suffit que $E_{10} \oplus E_{01} = K_1$. Lorsque cette condition est vérifiée, Q est multiplicative sur E et les trois formes sont multiplicatives sur E_+.

Preuve.

Soit e l'unité de E. Comme dans le cas commutatif, toute forme quadratique Q' multiplicative sur E vérifie l'une des conditions

a) $Q'(Y) = 0$ et $Q'(e-Y) = 0$

b) $Q'(Y) = 0$ et $Q'(e-Y) = 1$

c) $Q'(Y) = 1$ et $Q'(e-Y) = 0$

Q' est nulle sur les sous-espaces E_{10} et E_{01}. En effet, puisque $E_{10} = \{X \mid X \in E, YX = X \text{ et } X(e-Y) = X\}$, $E_{01} = \{X \mid X \in E, (i-Y)X = X \text{ et } XY = X\}$ $Q'(X) = Q'(Y)Q'(X) = Q'(e-Y)Q'(X)$ pour tout élément X de $E_{10} \cup E_{01}$. Puisque Q' vérifie a, b ou c, $Q'(X) = 0$.

- Lorsqu'une forme quadratique multiplicative sur E vérifie la condition (a), elle coïncide avec Q. En effet :

Puisque $Q(e) = Q'(e) = 1$, $Q'(Y) = Q'(e-Y) = 0 = Q(Y) = Q(e-Y)$, Q et Q' coïncident sur $E_{11} \oplus E_{00}$.

Q est nulle sur $E_{10} \cup E_{01}$ (prop. (4.3.1)'). Donc Q et Q' coïncident sur $E_{10} \cup E_{01}$.

$E_{10} \oplus E_{01}$ est orthogonal à $E_{11} \oplus E_{00}$ pour Q (prop. 4.3.1.'). D'autre part, pour tout élément X de E_{10}, $B'(Y,X) = B'(Y^2, YX) = Q'(Y)B(Y,X) = 0$ $B'(e-Y,X) = B'((e-Y)^2, X(e-Y)) = 0$. Donc E_{10} est orthogonal à $E_{11} \oplus E_{00}$ pour Q' de même E_{01} est orthogonal à $E_{11} \oplus E_{00}$ pour Q'.

Il reste à comparer $B(X,X')$ et $B'(X,X')$ pour X dans E_{10} et X' dans E_{01}. Soient $X_{10} \in E_{10}$ et $X_{01} \in E_{01}$. D'après le § 3 Chap. IV p. 104, $X_{01} X_{10} = - B(X_{10}, X_{01})(e-Y)$.

Puisque $Q'(X_{01} + Y) = Q'(X_{01}Y, Y^2) = 0$,

$$0 = Q'(X_{01} + Y)Q'(X_{10} + Y) = Q'\left[- B(X_{10},X_{01})(e-Y) + X_{01} + X_{10} + Y\right]$$

d'où compte tenu de ce qui précède,

$$0 = - B(X_{10},X_{01}) + B'(X_{10},X_{01}).$$

Toute forme quadratique multiplicative Q' qui vérifie (b) admet pour noyau $E_{11} \oplus E_{10} \oplus E_{01}$.

En effet, on sait déjà que les sous-espaces E_{11}, E_{10} et E_{01} sont totalement isotropes pour Q'. De plus, pour tout élément X de E_{10},

$$B'(Y,X) = B'(Y^2,YX) = Q'(Y)B'(Y,X) = 0$$

$$B'(e-Y,X) = Q'(e-Y)B'(e-Y,X) = B'(e-Y,(e-Y)X) = 0$$

Donc E_{10} est orthogonal à $E_{11} \oplus E_{00}$ pour Q'. De même E_{01} est orthogonal à $E_{11} \oplus E_{00}$ pour Q'.

D'autre part, pour tout élément X_{10} de E_{10} et tout élément X_{01} de E_{01}

$$Q'(X_{10} + e) = 1 \quad , \quad Q'(X_{01} + e) = 1$$

$$Q'(X_{10} + e)Q'(X_{01} + e) = Q'\left[-B(X_{10},X_{01})Y + X_{10} + X_{01} + e\right]$$

$$1 = 1 + B'(X_{10},X_{01})$$

Donc $B'(X_{10},X_{01}) = 0$.

Il reste à voir si inversement la forme Q' qui vérifie (b), $Q'(e) = 1$, et admet pour noyau $E_{11} \oplus E_{10} \oplus E_{01}$ peut effectivement être multiplicative.

Pour tout élément X_{10} de E_{10} et tout élément X_{01} de E_{01},

$$Q'\left[(X_{01} + Y)X_{01}\right] = Q'\left[-B(X_{10},X_{01})(e-Y) + X_{10}\right] = B^2(X_{10},X_{01})$$

$$Q'\left[(X_{01} + e-Y)(X_{10} + e-Y)\right] = Q'\left[-B(X_{10},X_{01})(e-Y) + e-Y\right] = B^2(X_{10},X_{01}) - 2B(X_{10},X_{01}) + 1$$

et $$Q'(X_{01} + Y) = 0 \quad , \quad Q'(X_{01} + e-Y) = Q'(X_{10} + e-Y) = 1$$

Donc pour que Q' soit multiplicative, il faut que pour tout élément X_{01} de E_{01} et tout élément X_{10} de E_{10}, $B(X_{10},X_{01}) = 0$. Ce qui implique que $E_{10} \oplus E_{01} = K_1$ (K_1 est le noyau de (E,Q), $E_{10} \oplus E_{01} = E'''$).

Inversement, il est immédiat que lorsque $K_1 = E'''$, Q' est multiplicative sur E. (Car E''' est un idéal bilatère contenu dans le noyau de Z).

En échangeant les rôles de Y et $e-Y$, on voit que toute forme quadratique multiplicative Q' qui vérifie (c) admet pour noyau $E_{00} \oplus E'''$ et que l'unique forme quadratique Q' qui vérifie (c), $Q'(e) = 1$, et admet pour noyau $E_{00} \oplus E'''$ est multiplicative sur E si et seulement si $K_1 = E'''$.

En définitive :

Lorsque $K_1 \neq E'''$, il existe au plus une forme quadratique multiplicative sur E. Lorsqu'elle existe, cette forme est la forme Q.

Lorsque $K_1 = E'''$, il existe exactement trois formes quadratiques multiplicatives sur E qui sont les trois formes multiplicatives sur E_+.

2 - Formes quadratiques multiplicatives sur une Q-algèbre alternative sur A lorsque A est intègre et $2 \neq 0$.

Proposition 5.3.2.-

On suppose A intègre et $2 \neq 0$. Soit E une Q-algèbre alternative sur A. On désigne par E_0 l'algèbre obtenue par extension des scalaires au corps des fractions A_0 de A, par Q_0 l'extension de Q à E_0 et par $K_{1,0}$ le noyau de (E_0, Q_0).

Il existe au plus trois formes quadratiques multiplicatives sur E. Lorsqu'il existe au moins deux formes quadratiques multiplicatives sur E, Q est multiplicative, K_1 est distinct de H (not. 0.1.2.) et $K_{1,0}$ est de codimension 2.

Lorsque de plus 2 est inversible dans A, il existe exactement zéro, une ou trois formes quadratiques multiplicatives sur E.

Lorsque les trois formes existent, elles sont également multiplicatives sur l'algèbre commutative E_+.

Preuve.

Une forme quadratique Q' définie sur E est multiplicative si et seulement si son extension Q'_0 à l'algèbre E_0 obtenue par extension des scalaires au corps des fractions A_0 de A est multiplicative.

Puisque E est alternative, E_0 est une A_0-algèbre alternative.

- Lorsqu'il existe au moins deux formes multiplicatives Q' et Q'' sur E, les extensions Q'_0 et Q''_0 de ces formes sont multiplicatives et distinctes sur E_0. Il existe donc une sous-algèbre de rang 2 de E_0 sur laquelle Q'_0 et Q''_0 sont distinctes, cette sous-algèbre est commutative, elle possède un idempotent

non trivial Y_0 (prop. 5.1.2., cor. 3). Donc d'après la proposition 5.3.1., E_0 possède trois formes quadratiques multiplicatives, $H_0 \neq K_{1,0}$ (donc $H \neq K$), $K_{1,0}$ est de codimension 2, Q_0 est multiplicative sur E_0 (donc Q est multiplicative sur E), et il existe au plus trois formes multiplicatives sur E.

- On suppose maintenant 2 inversible dans A. Lorsque $K_{1,0}$ est de codimension 2 et $H_0 \neq K_{1,0}$, E_0 admet un idempotent non trivial et $K_{1,0} = E_0''' Y_0$ (le raisonnement est analogue à celui de la preuve de la proposition 5.2.2.). Il existe donc sur E_0 trois formes quadratiques multiplicatives Q_0, $Q_0^{(2)}$ et $Q_0^{(3)}$ qui sont aussi les trois formes multiplicatives sur l'algèbre commutative $(E_0)_+$. Lorsqu'il existe deux formes multiplicatives sur E, ces deux formes sont multiplicatives sur E_+ car leurs extensions sont multiplicatives sur E_0 et $(E_0)_+$, il existe donc trois formes multiplicatives sur E_+ (prop. 5.2.4.). Comme leurs extensions sont multiplicatives sur E_0, ces trois formes sont multiplicatives sur E.

Références.

B. A. - BOURBAKI N.- *Algèbre.*

B. A. C. - BOURBAKI N.- *Algèbre commutative.*

[1] - BRAUN H. et KOECHER M.- *Jordan Algebren* (Springer 1966).

[2] - GOLDMAN O.- *Determinants in projective modules.* (Nagoya Math. J. 17-18 (1960-61)).

[3] - SCHAFER R.D.- *An introduction to non associative algebras* (Academic Press 1966).

[4] - SCHAFER R.D.- *Forms permitting composition.* (Advances in Mathematics, Vol. 4, n° 2 avril 1970).

[5] - BOREVITCH - CHAFAVERITCH.- *Théorie des nombres.* (G.V.)

[6] - HECKE E.- *Algebraische - Zahlen* (Chelsea).

TABLE DES MATIERES

Pages

CHAPITRE I : ALGEBRES UNITAIRES LIBRES DE RANG 2.

§ 1 - *Structures d'algèbre unitaire sur un A-module quadratique libre de rang 2.* 4

§ 2 - *Etude d'une algèbre unitaire libre de rang 2.* 8

CHAPITRE II : IDEAUX LIBRES DE RANG 2 D'UNE ALGEBRE QUADRATIQUE.

§ 1 - *Structures d'idéal d'algèbre quadratique sur un A-module quadratique libre de rang 2.* 28

§ 2 - *Correspondance entre classes d'idéaux et classes de formes quadratiques binaires.* 44

CHAPITRE III : ALGEBRES UNITAIRES DE RANG 2.

§ 1 - *Structures d'algèbre unitaire sur un A-module quadratique projectif de rang 2.* 56

§ 2 - *Etude d'une algèbre unitaire projective de rang 2.* 66

§ 3 - *Algèbres unitaires de rang 2 sur un anneau intègre.* 69

CHAPITRE IV : Q-ALGEBRES GENERALES.

§ 1 - *Propriétés préliminaires.* 84

§ 2 - *Q-algèbres associées à une forme bilinéaire symétrique.* 93

§ 3 - *Q-algèbres non nécessairement commutatives.* 107

CHAPITRE V : FORMES QUADRATIQUES MULTIPLICATIVES SUR UNE Q-ALGEBRE.

§ 1 - *Formes quadratiques multiplicatives sur une algèbre quadratique.* 115

§ 2 - *Formes quadratiques multiplicatives sur les Q-algèbres associées à une forme bilinéaire symétrique.* 123

§ 3 - *Formes quadratiques multiplicatives sur les Q-algèbres alternatives.* 132

*

* *